DOMESTIC THREAT INTELLIGENCE MANAGEMENT

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
GENERAL STUDIES

by

MARK A. JACKSON
B.S., Oregon State University, Corvallis, Oregon, 1989

Fort Leavenworth, Kansas
2001

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Mark A. Jackson

Thesis Title: Domestic Threat Intelligence Management

Approved by:

_____, Thesis Committee Chair
MAJ Charlotte R. Herring, J.D., L.LM.

_____, Member
LTC Mark A. Beattie, B.S.

_____, Member
Harold S. Orenstein, Ph.D.

Accepted this 1st day of June 2001 by:

_____, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

ABSTRACT

DOMESTIC THREAT INTELLIGENCE MANAGEMENT (DTIM) by MAJ Mark A. Jackson, USA, 109 pages.

This thesis examines DTIM at the US Army installation level. It reviews the Army's view of domestic threat based on current doctrine, as well as the joint view of terrorism as the predominate threat. It suggests a revised approach that fuses both Army and joint sources by combining the USACIDC's criminal categories with joint terrorism threat indicators. This model envisions threat as a hierarchy of seven criminal categories or *threat groups* ranging along a spectrum from terrorists to unsophisticated criminals. This approach accommodates the most dangerous threat scenario as well as focusing on a range of progressively more likely threat scenarios.

The thesis also examines current legal guidance for conducting DTIM. Although the Army is generally prohibited from conducting activities that may pervade civil law enforcement, there are narrow exceptions provided for activities that support a military nexus. As such, DTIM may be permitted in those situations with a clearly defined nexus. Research suggests, however, a need for establishing a more definitive and systematic process for determining this nexus.

Conclusions and recommendations are provided for developing DTIM to improve installation counterthreat measures. Hopefully, this thesis provides additional insight toward this goal and generates new ideas and areas for future research.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF ACRONYMS

AOR	Area of Operation
AR	Army Regulations
AT	Antiterrorism
DA	Department of the Army
DoD	Department of Defense
DTIM	Domestic Threat Intelligence Management
EECI	Essential Elements of Criminal Information
EOC	Emergency Operations Center
FM	Field Manual
FP	Force Protection
MACOM	Major Army Command
MDMP	Military Decision-Making Process
MP	Military Police
OOTW	Operations Other Than War
OSJA	Office of the Staff Judge Advocate
PIO	Police Intelligence Operations
PIR	Priority Intelligence Requirements
SASO	Stability and Support Operations
TREATCON	Threat Conditions
TTP	Tactics, Techniques, and Procedures
USACIDC	United States Army Criminal Investigation Command
USAMDW	United States Army Military District of Washington

CHAPTER 1

RESEARCH INTRODUCTION

> A broad range of criminal activities emanating from overseas threatens the safety and well-being of the American People.[1]
>
> The White House, *A National Security Strategy for a New Century*

Introduction

To accomplish the US national security strategy, the Department of Defense (DoD) must be capable of countering and defeating increasingly more innovative and mobile adversaries. A broad array of transnational dangers, including organized crime, illegal arms trading, and drug trafficking, pose a direct threat to Americans and American interests. Together with transnational criminals, terrorists pose asymmetric threats, such as cyber terrorism or sabotage, nuclear, biological or chemical weapons use, and other acts involving extreme endangerment. These risks--based on a high target probability--could potentially threaten the U.S. homeland.

Consequently, military requirements to support the security strategy have prompted a surge in antiterrorism and counterthreat initiatives for continental US-based military installations. This places new requirements on DoD to continuously evaluate threat and force vulnerability and to establish prudent countermeasures to mitigate potential risks. The DoD has responded to this challenge through an emphasis on "improved intelligence collection capabilities, heightened security awareness and force protection measures worldwide."[2]

Problem Background

Domestic threat intelligence support is a comprehensive, complex and resource-intensive mission. It involves the management of all criminal intelligence indicating a potential threat against domestic installations within the boundaries of the US and Puerto Rico. Many of its formal requirements are new and present a rather steep learning curve inhibited by a large number of issues. First and foremost, military police (MP) need time to absorb mission requirements and redistribute the necessary resources to develop mission parameters, requirements, and guidance. A glance at figure 1 reveals the shift in expectations for domestic intelligence from what was, traditionally, a military intelligence (MI) mission to one that has become predominantly an MP one. Unfortunately, MI's sudden departure left little continuity in a field already characterized by informal processes and conducted with only limited assets. As happens all too often, the shift in requirements was not accompanied with additional resources.

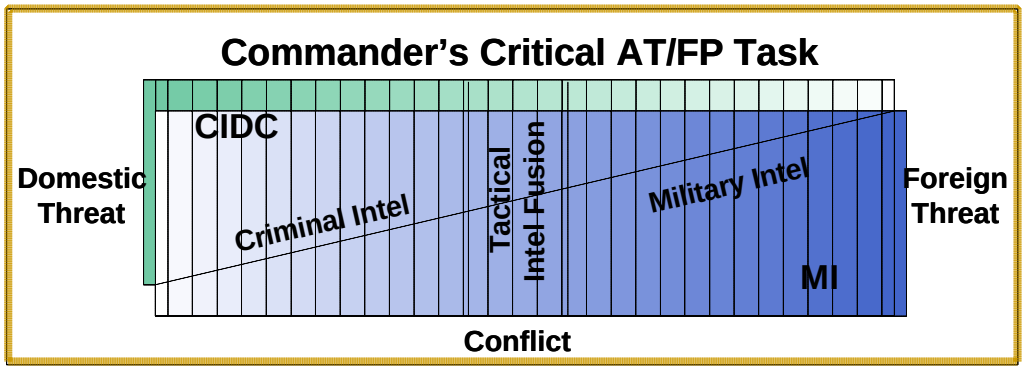

Figure 1. Intelligence Workload Distribution

The MPs must develop new systems to accommodate an assortment of other issues. They must sort through the complex legal implications associated with collecting

intelligence in a domestic environment, possibly against US citizens. This requires the development of new or improvement of existing intelligence networks with federal, state, and local civilian law enforcement for domestic intelligence support. Work in this area also requires procedures for ensuring close coordination with the Office of the Judge Advocate General (OTJAG) and systems for gauging and monitoring legal liability against domestic threat intelligence management (DTIM) restrictions.

Application systems, too, are essential to shore up gaps created by new demands for intelligence products. The MPs must develop a thorough understanding of how they support installation security and force protection. This means that DTIM must be capable of providing standard intelligence products to installation commanders and other agencies requesting support. Products must provide a clear picture of potential threats at the local level, while at the same time, providing a formal and standard product for the Department of the Army (DA), Major Army Commands (MACOM) or other agencies requiring a standard assessment across numerous or all-domestic installations.

Moreover, there has been an internal movement of late, focusing on the use of criminal intelligence in the nondomestic tactical environment. The Army's increasing operations tempo toward peace operations and other lower-scaled intervention has placed new emphasis on reducing criminal activity as a required part of stabilizing an area of operations. In response, the Military Police Corps has recently reviewed its traditional battlefield functions, leading to several substantial changes, including the new mission of police intelligence operations. Such a firm commitment toward conducting police intelligence operations--specifically, criminal intelligence--has created institutional

pressure to develop and publish new policies and procedures for managing threat intelligence.

Similar to the development of any new doctrine, missions, or regulatory guidance, Army law enforcement will require time and resources to sort out the vast number of challenges affecting DTIM operations. Progress in this area will require a comprehensive review of current practices, an assessment of success and shortcomings, and the development of guidance based on findings. At best, it will be an evolutionary process characterized by incremental improvement. Each step toward improving DTIM operations must consider the last step before designing the next. By examining some of the current features of DTIM operations to develop some proposals for future adoption, this paper represents one such step.

Primary Question

How should Army law enforcement legally conduct DTIM and apply it to assess the domestic threat against continental US installations?

Related Subordinate Questions

How should domestic threat be defined?

How will the Army use DTIM to assess the threat and how will threats be categorized (see definitions)?

What are the legal liabilities or restrictions of conducting DTIM within the boundaries of the US and Puerto Rico?

How will DTIM processes support force protection and security systems for installations?

How will DTIM processes parallel criminal intelligence processes in a tactical environment?

Answering the primary question provides several unique challenges: (1) developing "how to" conclusions in a relatively parochial and unpublished field, (2) consolidating and integrating several areas (e.g., intelligence, security, force protections) into a single set of criteria for forming conclusions, and (3) developing criteria to sort through the oral "how to" traditions for valid concepts. Nevertheless, any answers may have important application to Army law enforcement and lower-scale military operations. At the end of the day, they could provide a platform from which to springboard future research and development.

Background

Limited Use of Military for Domestic-Civil Intervention

As a DoD member, the Department of the Army shares a portion of the strategic role to defend the homeland and population. When called upon, it can unilaterally defend against any type of invasion by a foreign threat or other military force, but, when necessary, it can also defend against internal threats deemed beyond the capability of civil authorities. Defense against internal threats--as it pertains to enforcing civil laws--is severely restricted by the Constitution, US law (Posse Comitatus Act), and American traditions dating back to the post-civil war restoration period.[3] However, "there are two constitutional exceptions, based on the legal right of the United States to guarantee the preservation of public order and the carrying out of governmental operations . . . by force if necessary."[4] The first exception is granted by "emergency authority," which permits use of the Army in situations when "civil disturbances, disasters, or calamities seriously

endanger life and property and disrupt normal governmental functions."[5] The second exception provides the Army with the right to protect federal property and military functions (Army missions):

> The right of the United States to protect federal property or functions by intervention with federal military forces is an accepted principle of our government. The right extends to all federal property and functions wherever located. This form of intervention is warranted, however, only where the need for protection exists and local civil authorities cannot or will not give adequate protection.[6]

There are also two "common law" exceptions. The first allows a military member to act as private citizen in defending against internal threats or otherwise supporting civil authority. This parallels other rights retained by a military member when acting as a private citizen, notwithstanding his military status.[7] The second exception is captured under "Military Purpose Doctrine" and grants the Army the ability to assist civil authorities in pursuit of a military purpose, so long as any benefit to civil authorities is only incidental. An example here might involve the use of MP explosive-detector dogs at an off-post school attended by military family members. The purpose is to protect military family members, but the fact that it also protects community children and nonmilitary property is an incidental benefit to local civil authorities.

Perhaps the most important and the least understood of these four exceptions involves the Army's right--and responsibility--to defend against internal threats based on the constitutional exception to "protect federal property and functions," and the common law exception to assist civil authorities to achieve a "military purpose." Although these exceptions may grant commanders generous latitude to establish security on continental US installations, interpretation of such permissions off of the installation remains

somewhat confusing. These exceptions, nevertheless, may provide some important inroads for granting installation commanders the ability to influence the threat environment beyond the installation's borders.

Protecting the Domestic-Based Army

Despite the underdeveloped nature of domestic security, the Army has an inherent responsibility for providing defense of continental US based installations, including Alaska, Hawaii, and Puerto Rico. In fact, "Title 10, USC requires that the Army issue regulations for the safety of its people and the preservation of its property."[8] Responsibility for implementing these regulations is normally delegated to installations, but can flow to every level that, as a practical matter, governs custody, use, and preservation of force protection objects (i.e., critical resources, personnel, and information).[9] As of 1999, installation security has become the focus of Joint Service Installation Vulnerability Assessment teams working with commanders and staff to assess baseline compliance, to document new developments, and to educate commanders and their staff.

At a minimum, security should protect critical resources on the installation (including real property), sustain mission objectives, safeguard persons assigned or visiting the installation, and secure military information. These responsibilities may range anywhere from protecting classified information to securing weapons to interdicting drug trafficking, or may even include highly specialized missions, such as security support for the US President, US and foreign dignitaries, the Secretary of the Army, or other high-ranking military officials meeting or visiting in or around the installation or within its specified jurisdiction.

Depending on local threat conditions, installation commanders and staff may also have additional security responsibilities. To determine these requirements, the installation staff must assess the effect of local threat conditions on the security of the installation. The assessment should consider three threat factors: (1) missions or contingency plans supported by the installation, (2) the effects of local threat to installation interests, and (3) the unique "target value" of force protection objects associated with the installation. (Although not doctrinal, the latter term refers to the specific incentive value that a particular installation, activity, person, or information may present to a criminal or criminal organization, whether it is monetary, recruitment, power, prestige, or of other symbolic value.)

Based on these threat factors, a local threat assessment usually provides a threat picture specific to a single installation or grouping of installations. This means that each installation may have specific security requirements tailored to its individual assessment. (One exception to this specificity was the 1998 force protection mandate requiring all continental US installations to establish threat condition (THREATCON) A-plus status, in response to terrorist attacks on American Embassies in Africa.) As assessments are updated, security requirements continue to change to reflect the change in threat conditions. This constant change acts to reinforce installation specificity and as a result, has dampened initiatives toward standardizing threat countermeasures, except in the broadest sense, such as those found under published THREATCON. But even THREATCON measures can be tailored to address unique security requirements, such as blending particular measures from THREATCON A and B to arrive at A-plus as illustrated in the aforementioned example.

Example of Organizational and Installation Specificity

The US Army Military District of Washington (USAMDW), which often conducts nationally viewed events in and around the nation's capital, provides an example of organizational/installation specificity. Its distinctive designation: "Guarding the Nation's Capital," explicitly denotes an inherent security mission that clearly distinguishes it from other comparable organizations. Because of the strategic environment, unique missions, and higher-range target values, missions within USAMDW often require security planning and execution well beyond the Army's more routine force protection responsibilities. Also, its mission statement entails some additional implicit security requirements:

> The US Army Military District of Washington is a unique Army command which, while covering a small geographic area for a major Army command, has an important mission which is threefold:
>
> Respond to crisis, disaster or security requirements in the National Capital Region (NCR) through implementation of various contingency plans
>
> Conduct official ceremonies and public events, locally and world-wide on behalf of the Nation's civilian and military leaders
>
> Provide base operations support for U.S. Army and Department of Defense organizations throughout the NCR and New York City. Provide a variety of specialized support including personal property shipping and storage services for the region, rotary-wing airlift, and operation of the Arlington National Cemetery[10]

As the home of the 3d US Infantry (The Old Guard), this MACOM has explicit responsibilities for supporting security for a wide range of domestic and foreign dignitaries visiting or meeting within US Army jurisdiction or conducting activities requiring Army support (e.g., wreath ceremonies in Arlington National Cemetery, presidential inaugurations, state funerals, etc.). Fort Myer, an installation within USAMDW, is also the home for some of the military's most senior community residents,

including the Chairman of the Joint Chiefs of Staff, service chiefs, and numerous general officers. Their presence, combined with numerous distinguished domestic and foreign visitors, often adds an additional security dimension to mission planning and execution. Such conditions offer an example of how threat factors at Fort Myer may create a different threat condition than at other less conspicuous installations. When added to the general flux in threat conditions created by changing threat factors (e.g., an increase in the installation's threat value by the arrival of a foreign prime minister), security planning can become a complex and resource intensive process.

Using Intelligence for Installation Security and Force Protection

To effectively manage the shifting nature of threat conditions, commanders must plan, prepare, and prioritize installation countermeasures. This commitment requires an understanding of the threat environment at the strategic, operational, and tactical levels. Developed from top to bottom, commanders must have a picture of global security concerns and current threats against US domestic interests, potential threats to DA and domestic installations, and threats emanating from within their local environment. They must also take into account the security resources and external support available, decide on the appropriate security tasks, and plan and implement the necessary measures to counter threats against "force protection objects," critical resources, personnel, and information.

This requires installation commanders to make calculated decisions on how to balance security and the interruptions and inconveniences associated with it with routine operations, services, and missions. By clearly understanding the type, intent, and capabilities of the threat, commanders and staffs can effectively plan and implement

countermeasures that will deter, detect, detain, or defeat the particular threat, without imposing undo hardship on installation service providers and customers. In each case the value of the countermeasure must be measured against the benefits gained.

Implementing entry control procedures, for instance, is a popular countermeasure against most external threats, but because it is extremely resource intensive and can be disruptive to routine operations, services, and missions, its costs may outweigh the benefits in preventing certain threats. Increased entry control requires increased manning (many personnel are often pulled from other important jobs or functions), generates delays for installation commuters, and can create dangerous traffic conditions. Against low or negligible threats, such costs may not be justified. Even when employed against midlevel threats (e.g., drug traffickers or gang recruiting), entry control measures can be tailored to better support routine operations.

Intelligence plays a vital role in these processes. The *Military Requirements of the Defense Strategy* highlight the importance of using intelligence: "Because intelligence represents the first line of defense, DoD has implemented procedures to improve its collection and use of terrorism-related intelligence, getting the needed product into the hands of the local commander as rapidly as possible."[11] It allows commanders to develop a clear picture of potential threats against their installation and generate appropriate countermeasures. It also helps them to build successful force protection programs by refining security processes through improved security planning, security and response training, crisis and consequence management, and resource economy.

The latter process is perhaps the most important. In an environment characterized by dwindling resources, intelligence can economize resources by limiting false responses,

minimizing strategic consumption, and allowing resource sharing among installations. Intelligence can help prioritize the security workload in several ways. First, by tailoring security toward actual threats, intelligence ensures that an installation does not react to one threat with the tactics, techniques, and procedures (TTPs) for another, nor waste resources implementing counterthreat measures against nonexistent threats. Second, it allows commanders and staffs to evaluate and allot resources; it allows commanders to counter more dangerous threats, mitigate lesser threats, and accept risks associated with negligible threats. Finally, just as intelligence can identify and prioritize threats, it can also confirm the absence of threat, allowing installations to share resources when and where appropriate. Similarly, it helps higher headquarters to prioritize support and resources across numerous subordinate organizations and installations.

Defining Domestic Threat Intelligence Management

Although the field of intelligence has broad applications and is characterized by a plethora of terms, many of them interchangeable or describing slight nuances, the definition of Domestic Threat Intelligence Management (DTIM) has important implications toward its conduct. The US Army Criminal Investigation Command (USACIDC) currently defines DTIM as "intelligence relating to criminals, crimes, or activities or conditions within the United States that pose a threat to internal security."[12] With the exception of some minor adjustments, this definition has suitable application for the study of DTIM processes. Adjustments to the definition should expand the jurisdiction of DTIM operations to include Puerto Rico, while limiting its military application to include only those threats against DoD interests. These adjustments provide a revised definition of domestic threat intelligence for purposes of this thesis as

"intelligence relating to criminals, crimes, activities or conditions within the United States and Puerto Rico that pose a threat to DoD interests." Domestic threat intelligence management, then, simply describes the management processes involved in collecting, processing, disseminating, and storing domestic threat intelligence as it relates to domestic installation defense and with respect to its legal parameters.

This definition provides a straightforward approach to the application of DTIM, emphasizing three important points worth highlighting: (1) threat is associated with crime and not some other accident, incident, or natural disaster; (2) for intelligence processes relating to the military, threats must pertain to DoD interests; and (3) threats must affect those interest within the domestic environment. The first point establishes a clear link between threats and criminal activity or conditions. This linkage broadens the scope of threat intelligence from a more traditional focus on terrorism, to include a full range of "threat groups" comprised of seven categories: unsophisticated criminals, drug traffickers, gangs and hate groups, extremists, organized criminals, saboteurs, and terrorists. This important distinction is discussed in chapter 4.

The second and third points set the stage for the current status and challenges confronting DTIM operations. They describe DTIM as intelligence operations conducted by the military for the security of DoD interests within a domestic environment. Similar to the limitations discussed under subheading "Limited Use of Military for Domestic-Civil Intervention," the military is severely limited to conducting intelligence--DoD interests, notwithstanding--against US citizens in a domestic environment.

This limitation stems from DoD Regulation 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*

*a*nd precludes MI elements or organizations from conducting intelligence operations targeting US citizens.[13] This limit severely restricts an MI element's ability to provide threat intelligence in support of domestic-based installation defense. Although it may provide or share intelligence linking foreign threats against domestic targets or any intelligence relating to members of the military community, it is clearly prohibited from conducting intelligence operations regarding domestic threats originating off the installation.

An exception to this mandate, however, is provided for domestic threat intelligence operations conducted in association with law enforcement operations. Under certain conditions and in compliance with certain criteria--less restrictive than those imposed on MI--military police can provide DTIM in support of domestic-based installations. In cases where there is a clear military nexus (e.g., conditions established by military purpose doctrine, or within the Army's charter to protect federal property and functions, etc.), for instance, MPs can provide domestic threat intelligence on US citizens.

Combined with increased pressure for improving Army compliance with DoD Regulation 5200.27--certainly nudged by dwindling resources and competing commitments--the law enforcement exception established the groundwork for the eventual withdrawal of MI in February 1999 from providing DTIM support for domestic security and force protection initiatives.[14] To fill the subsequent gap, the Army repositioned the requirement to the MP and, in particular, USACIDC. As a result, USACIDC's DTIM requirements dramatically increased to cover obligations traditionally supported by MI.

Energized by a recent focus on domestic security, such as the 1998 THREATCON upgrade to Alpha-plus or the Federal Bureau of Investigation's 1999 report on millennium-related domestic threats, the shift toward formal DTIM support will create new and recurring challenges for MPs and USACIDC units. This trend promises continual growth as more and more customers request subsequent DTIM support for installation security and force protection. To manage these new and overwhelming requirements, MPs must develop new standard processes to improve the efficiency and effectiveness of DTIM.

Research Outline

The research outline is comprised of three distinct sections as presented below. Each section provides discussion based on research and experience concerning potential gaps in current DTIM operations. The first two sections focus on how the Army views and determines domestic threat, and what the legal considerations are in conducting intelligence against such threats, respectively. The third section uses a USACIDC DTIM model to discuss how conclusions from the first two sections might be implemented into current DTIM processes.

Section I. Determining Threat

The first section includes a discussion of the military's view of terrorism, its emphasis on terrorism as the primary threat, and the current method for determining the threat level. It discusses the appropriateness of such a singular emphasis on terrorism. Why, for instance, is terrorism emphasized almost to the point of excluding other criminal categories? What is the difference between this form of crime and others? Should current threat processes include other forms of criminal activity and, if so, which

ones? This section proposes some answers to these questions and offers a potential solution to determining the threat. In addition to terrorism, it discusses six additional criminal categories or threat groups and presents a more balanced view with respect to the "worst versus most likely scenario" of potential domestic threats. Finally, it expands current methodology for determining terrorist threat levels to develop and propose a new model for determining threat across the full spectrum of threat groups.

Section II. Defining Legal Parameters for Conducting DTIM

The second section reviews the legal implications of conducting DTIM. As discussed herein, this area has perhaps the greatest impact on military operations in the domestic environment, yet it remains one of the most underdeveloped areas affecting DTIM. Although progress has been slow in coming, this area continues to evolve. The court appellate system continues to interpret the parameters of military law enforcement with respect to US citizens on a case-by-case basis. When applied to current law and regulatory guidance, appellate decisions can provide key insights that may expand, contract, or maintain the status quo of current military law enforcement processes. Regardless of case outcome, court findings provide an ever-changing process for evaluating, assessing, and adjusting current regulations governing the legal conduct of the military's domestic law enforcement. Although a review of hundreds of appellate cases revealed only a negligible impact on DTIM operations, an impact, nevertheless, may exist based on the relationship between DTIM and domestic law enforcement. Since DTIM parameters parallel those of domestic law enforcement, any progress in one field should relate to the other. This premise is bolstered by a few examples of recent appellate decisions that may indirectly affect the legal guidelines for conducting DTIM.

Finally, this section reviews current legal parameters for conducting DTIM and proposes a new model for determining a military nexus. This model suggests a systematic process for organizing and prioritizing essential elements to determe a military nexus. It also provides metrics for evaluating the potential legal liability involved with domestic operations.

Section III. Conducting Domestic Threat Intelligence Management

The last section outlines how DTIM supports installation security and force protection. It includes a review of some of the latest efforts to refine threat intelligence operations with respect to general guidance provided by DoD and joint publications. Although only a cursory review, it covers current progress in standardizing and improving DTIM processes. This section highlights the USACIDC's "Domestic Threat Intelligence Management Model," which represents an important contribution in this effort.[15] The model portrays DTIM as a continuous cycle, organized into four phases: (1) *Intelligence Collection* to identify threats, provide advance warning, and disseminate threat intelligence; (2) *Threat/Vulnerability Assessment* to measure potential strengths and weaknesses in installation defenses; (3) *Crisis Management*, which relies on real-time intelligence for incident response and mitigation; and (4) *Analysis and Deterrence*, which uses intelligence for investigating, reporting, and capturing lessons learned. This section also discusses essential law enforcement, security, and intelligence agencies involved throughout this process.

Limitations

The most severe constraint associated with this topic is the lack of literature covering DTIM operations. Although there are numerous publications covering criminal

intelligence from within the law-enforcement community (federal, state, and local), there is very little literature concerning the specific challenges facing military law enforcement. Unlike other law enforcement agencies, military law enforcement is confronted by tighter restrictions on collecting intelligence on American citizens not affiliated with the military. This restriction is central to the thesis and requires much attention in answering the primary and secondary questions.

Delimitations

This thesis will not address the analysis of information or intelligence. There is a plethora of literature concerning this topic and, although there is very little published within the military law-enforcement community, intelligence analysis for DTIM parallels intelligence procedures elsewhere. Also this thesis will not attempt to provide a definitive source for conducting DTIM operations. Instead, it will focus on those areas that may present a particular challenge to conducting DTIM, in an attempt to provide insight and general guidance. Finally, although this thesis includes some new models that propose new methodology for overcoming several facing DTIM operations, testing the validity and reliability of these models is beyond its scope. The intent of the models is simply to suggest new methodology and provide a forum for further inquiry.

Definition of Terms Used

The following terms are defined.[16]

Criminal Activity Threat Assessment (CATA). Organized intelligence efforts by USACIDC to determine the criminal threat for a general area of concern or a specific contracted event (when the event is scheduled within six months of the assessment). A CATA is a written product that is tasked and suspensed by JSIVA when it will be used as

a preoperation brief to JSIVA, and it is tasked and suspensed by DAMO-ODL when it is conducted for a specific contracted event.

Criminal Activity Threat Estimate (CATE). Organized intelligence efforts by USACIDC to determine the criminal threat for a specific event (when the event is planned six months or more from the assessment). The CATE is tasked and suspensed by DAMO-ODL. It acts as a prelude to the CATA and is normally not as involved or detailed. The CATE is simply a general estimate of criminal activity and its potential impact on the upcoming event. Input may be provided by telephone or electronic mail.

Commander's Force Protection Critical Tasks. A comprehensive list of requirements identified by the commander as being critical in facilitating timely force protection management and the decision making process that affect successful force protection accomplishment (see figure 2).

Criminal Intelligence. The product(s) that result from the collections, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities of supported organizations.

Domestic Threat. Terrorism or criminal threat perpetrated by the citizens of one country against fellow countrymen. That includes acts against citizens of a second country when they are in the host country, and not the principal or intended target.

Domestic Threat Intelligence. Intelligence relating to criminals, crimes, or activities or conditions within the US that pose a threat to internal security.

Domestic Threat Intelligence Management (DTIM). Established procedures for managing information collection and intelligence processing, dissemination, and storage.

Domestic Threat Intelligence Management Model. A USACIDC model that synchronizes intelligence management through four phases of USACIDC force protection support, including: threat assessment, vulnerability assessment, crisis management, and analysis and deterrence.

Extremist Criminal Activity Threat Assessment (ECATA). An annual USACIDC tasking conducted at each field element in the format of a crime analysis survey, targeting actual or suspected criminal activity committed by extremist groups (including gangs). The ECATA of each field element is compiled, collated, and summarized at USACIDC, with the findings reported to the Secretary of the Army.

Economic Crime Threat Assessment (ECTA). Economic intelligence that is normally compiled on a continuous basis and reported to USACIDC annually. Its purpose is to assess the economic crime threat to Army property, funds, and personnel within a specific area of responsibility (AOR) and to prioritize the identified targets.

Essential Elements of Criminal Information (EECI). The EECI is a method of targeting information collection efforts at specific criminal activity within USACIDC's area of investigative responsibility. The EECI will be prepared so that the recipient is able to focus upon specific items of inquiry during a collection window. Normally, EECIs will be issued either by USACIDC, or by a USACIDC major subordinate command.

Force Protection. Security program designed to protect service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by

intelligence, counterintelligence, and other security programs. A diagram of current force protection doctrine is at figure 2.

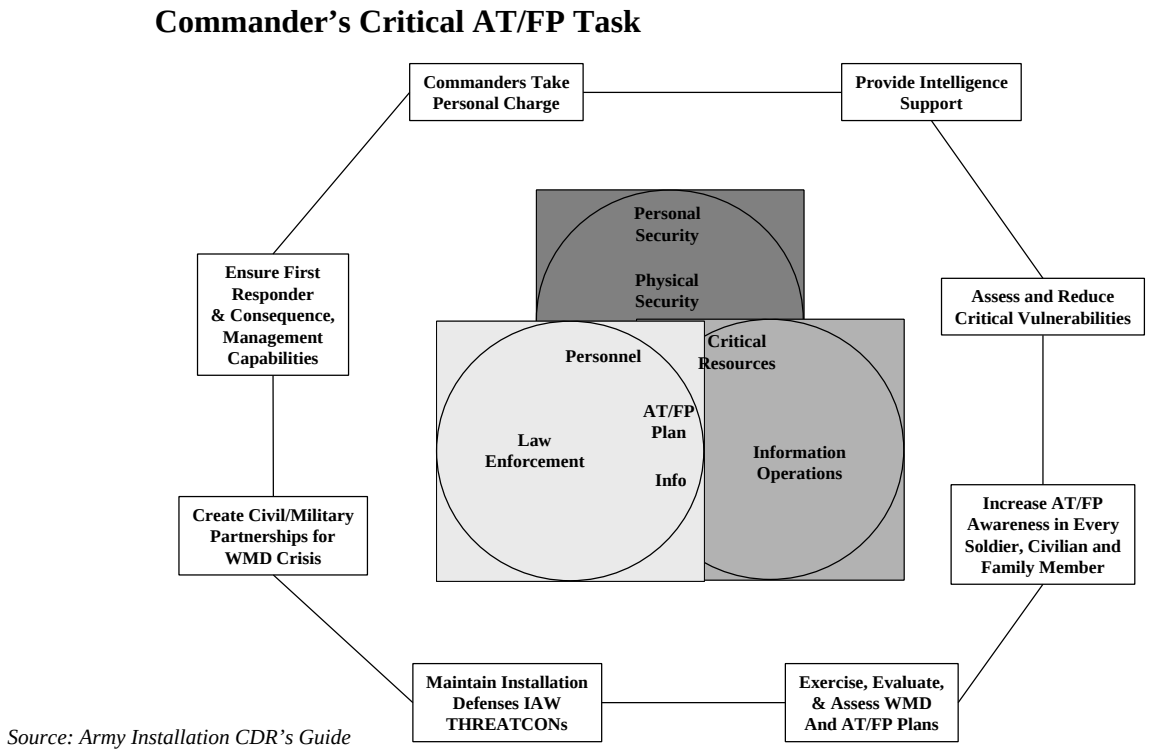

Figure 2. Force Protection Doctrine, Installation Commanders' Antiterrorism Guide

Force Protection Objects. The potential target of a terrorist attack (i.e., personnel, critical assets, or information).

Force Protection Program Elements. Subprograms of force protection designed to protect FP objects (i.e., personal security, physical security, law enforcement, and information operations). Program elements are supported by the synchronization of doctrine, training, operations, intelligence, and resources.

Intelligence. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information.

Joint Services Integrated Installation Vulnerability Assessments (JSIVA) Team. A team under the Defense Threat Reduction Agency (DTRA) charged with providing independent assessment capabilities to the CINCs, services, and agency directors, along with technical expertise and assistance in meeting force protection standards. This team provides installation commanders on-site assessments by examining the vulnerabilities to potential terrorist attack and other threats within its area of responsibility.

Military Nexus. A means of connection, link, or tie to the armed forces through either the status of the offender, intent of the crime or threat, or the location of the event.

Priority Intelligence Requirements. Intelligence, which is crucial and requires the immediate attention of the commander. It enables the commander to make decisions that will provide a timely and appropriate response to actions by a potential/actual enemy

Personal Security Vulnerability Assessment (PSVA). An assessment designed to enhance the overall security posture of selected individuals, normally conducted for general officers and other high-risk personnel.

Terrorism. The calculated use of violence or the threat of violence to attain political, religious, or ideological goals. Terrorists intimidate, coerce, and instill fear. Terrorism involves a criminal act that is often symbolic in nature and intended to influence an audience beyond the immediate victims.

Threat Conditions (THREATCON). Four THREATCONs Above Normal:

1. THREATCON ALPHA: This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of

THREATCON BRAVO measures. The measures in this THREATCON must be capable of being maintained indefinitely.

2. THREATCON BRAVO. This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

3. THREATCON CHARLIE: This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel facilities and is imminent. Implementation of measures in this THREATCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

4. THREATCON DELTA: This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely.

---

[1]The White House, *A National Security Strategy for a New Century* (Washington DC: The White House, December 1999), 15.

[2]Ibid., 24.

[3]US Department of the Army, US Marine Corps, FM 100-19, FMFM 7-10, *Domestic Support Operations* (Washington, DC: US Government Printing Office, July 1993), 3-0. Constitutional limitations refer to the principle subordinating the armed forces to civilian authorities (US Constitution, Article I, 8, cl. 11-12). As to Posse Comitatus, the Judiciary Act of 1789 allowed US Marshals to request military forces as a posse. During the Reconstruction Period, however, local and national southern politicians considered use of the military for such purposes abusive. Consequently, President Rutherford B. Hayes signed a bill abolishing its practice. It is currently contained within 18 USCS 1385 as:

Whoever, except in cases and under circumstances expressly authorized by the Constitution or act of Congress, willfully uses any part of the Army or the Air Force as a Posse Comitatus or otherwise to execute the laws shall be fined not more than $10,000 or imprisoned not more than two years, or both. (FM 100-19, 48).

[4]Mathew J. Gilligan, "Opening the Gate," *Military Law Review*, vol. 161, (September 1999),12.

[5]Ibid., 14. Emergency authority has expanded in the last few decades to include a wide range of activities including drug interdiction, fighting forest fires, conducting illegal immigration internment, etc. The caveat to this exception is outlined in AR 500-51, para. 3-4b(1), which limits military intervention to only those situations wherein "local authorities are unable to control the situation."

[6]Title 5, USC, 301 (1998).

[7]"Opening the Gate," 35. Individual rights in this case, refers to those rights granted to any citizen regardless of military status. The citizen's arrest provides the best example of this type of exception. Although an officer outside of his jurisdiction would not have any rights or authority inherent with his position, he would possess the rights that are granted to any citizen of that state, including the right to perform a citizen's arrest. This right as been affirmed in several court cases involving military law enforcement off the installation.

[8]Title 10, USCS.

[9]Critical resources, personnel, and information are referred to as "Force Protection Objects" in the *Installation Commanders' Antiterrorism Handbook*. New and emerging doctrine in this area has provided a variety of concepts and vocabulary including those associated with the terms "Force Protection" and "Protecting the Force." For purposes herein, the term force protection objects simply provides three categories of threat targeting: personnel, critical resources, and information. For instance, a threat group may target an installation or other real property, personnel (whether on or off the installation), or information for theft, assault, vandalism, recruiting, etc. The object of "information" may conger up images of the high profile crime alleging Chinese espionage of US nuclear secrets at Los Alamos, NM, in February 2000.

[10]US Department of the Army, "U.S. Army Military District of Washington Homepage" [on-line]; available from http://www.mdw.army.mil; Internet; accessed on 5 February 2001.

[11]The White House, 26.

[12]US Department of the Army, United States Army Criminal Investigation Command, Operations Memorandum 002-00, *Force Protection Initiatives and Domestic Threat Intelligence Management* (Fort Belvoir Va: USAUSACIDCC, February 2000), A-2.

[13]US Department of Defense, DoD Directive 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense* (Washington, DC: US Government Printing Office, no date).

[15]USACIDC Operations Memorandum 002-00, 3.

[16]Ibid., App A. While working as the Chief, Criminal Intelligence Branch for Headquarters, USACIDC, this list of "definitions of terms" was put together using various sources to standardize terminology within the command. In some cases, terminology represents several joint, DoD, or Army sources and in other cases, it was developed specifically by USACIDC for use within the command. The Deputy Chief of Staff for Operations, USACIDC, approved this list of definitions for USACIDC. Although this thesis only mentions several of these terms they are included to provide some insight into the latest work in this area.

CHAPTER 2

LITERATURE REVIEW

> The US Government must not trample on American lives and liberties in the name of preserving them. The military will not exceed legal authorities when performing a counterterrorism mission.[1]
>
> Secretary Cohen, *Preparing for a Grave New World*

Introduction

The purpose of this chapter is to provide a review of the literature relating to how the Army should conduct DTIM operations. This chapter examines the patterns of literature that have emerged in the last couple of decades to both expand and limit DTIM. It includes those few milestones that have prompted institutional pressures for providing DTIM related services, but also addresses the lack of supporting literature for providing "how to" systems and processes. This chapter also discusses the growing trend in Army literature toward the generalization of threat and an opposing trend by joint doctrine toward a more specific characterization. It will include a look at doctrine that pertains to threat within the domestic environment, as well as those operations countering parallel threat in external environments. Finally, it reviews USACIDC's latest work to address some of these issues in its publication of Operations Memorandum 002-00, *Force Protection Initiatives and Domestic Threat Intelligence Management* in early 2000.[2]

Although very little has been published that specifically addresses DTIM per se, there are several literary categories that cover related areas or that implement or parallel certain aspects of DTIM operations. It is worth noting here, however, that since most of these sources require some level of interpretation to identify their relationship to DTIM,

many observations and conclusions based on these sources may require rather broad generalizations, and, in a few cases, a leap of faith. Overcoming this limitation, nevertheless, may prove necessary as the first step in providing the groundwork for developing DTIM. Whether or not one agrees, any reaction may catalyze publications that are more direct in nature.

Influence of Politics and Media

Almost any strategic-level defense, security, or military document includes an important topic related to DTIM. Some of these sources include *A National Security Strategy for a New Century*, the *National Defense Strategy*, the *National Military Strategy*, the *United States Army Posture Statement FY01*, and a host of other parallel or supporting documents. Whether they are referring to homeland defense, transnational threats, terrorism, drug trafficking, international crime, domestic preparedness, weapons of mass destruction, or another *buzzword* of late, they are undoubtedly focusing on threats or threat effects against the domestic environment. The gist of their messages is essentially the same: internal and external threat groups are on the rise, their capabilities are advanced, and they will leverage technology and destructive weapons to gain asymmetry. This passage from *A National Security Strategy for a New Century* provides an example of these literature sources:

> Our potential enemies, whether nations or terrorists, may be more likely in the future to attacks against vulnerable civilian targets in the United States. At the same time, easier access to sophisticated technology means that the destructive power available to rogue nations and terrorists is greater than ever.[3]

Although not prescriptive per se, these documents provide the source for the military's emphasis on domestic threat. As such, these political-military documents

provide the impetus for Army's domestic security, to include both, potential support to civil authorities and domestic installation security. While some sources refer to the need to increase law enforcement vigilance or intelligence capabilities, for most it is an implied task. Consequently, any reference to DTIM activities within these documents remains general or unspoken.

The emphasis on domestic security has also been a hotly debated topic in Congress. The military's role, with respect to the implications of laws and traditions limiting its involvement in civil affairs, has provided the media with a readily available source of controversy. There are a plethora of articles documenting this controversy, especially during times of or associated with a domestic threat or terrorist incident, such as the Oklahoma City bombing or the attack on the USS *Cole*. In addition to covering political trends in this area, media stories also provide a good sensing of the level of interest and sensitivity to domestic threat and the military's role in countering it. The effects of the media on civil-military cooperation and, specifically, DTIM, however, are beyond the scope of this research. Media articles herein are only cited with reference to their content.

Prior Research

The second category addresses prior research. No level of query, not traditional library systems, not subject matter experts, not even the Internet, could provide a single source--beyond a memorandum published by CID--specifically addressing DTIM operations within the Army. This discovery comes as no surprise. It was a fact that was presented in chapter 1 as an anticipated problem. Unfortunately, the application of

military threat intelligence in the domestic environment has been predominantly an informal process.

The other categories, therefore, are introduced and discussed as they generally relate to certain aspects of DTIM. Because of the often-speculative nature of indirect sources--controversy or flawed logic, notwithstanding--a discussion of these categories in this chapter and subsequent ones will attempt to borrow from the primary imperative of psychology: "first, do no harm." In developing the relationship between parallel or associated research, discussions will endeavor to avoid confusing concepts or terminology. Instead, discussions will use existing terms and principles where applicable, clearly establish the premise for necessary modifications, or address the more complex interpretations (and all leaps of faith) as a part of the endnotes. Any newly created terms or principles will be developed using the most current information available. Although there is little guidance in the way of domestic threat intelligence, it is important not to violate any standing terms, principles, or "how to" methodology, without due consideration and explanation. Unless making a connection between this thesis and a related topic, regulations, field manuals (FM), and policies will be utilized within their stated parameters, be it intelligence, force protection, or other related topics.

Threat Doctrine

The third category of literature relates to those doctrinal sources that can be lumped together under "threat" literature. These primarily include the two separate trends offered by Army and joint doctrine. As it pertains to threat, Army doctrine can be further subdivided into "administrative" and "operational" literature. The distinction between these classifications simply separates threat literature by its association with

Army operations or by its association with administrative programs. Operational literature covers those threats that are discussed as a part of doctrine associated with a wide variety of operations throughout history, including small wars, operations other than war (OOTW), peace operations, stability operations, support operations, and countless other types. Administrative threat literature, on the other hand, covers Army programs or program requirements with respect to threat guidance, operations, and policies. This includes all threats that are countered by such programs as force protection, security, physical security, loss prevention, crime prevention, and numerous others.

While the distinction between operational and administrative literature may readily align itself to the traditional separation between garrison and tactical environments, that is not their distinguishing feature. In fact, as Army operations have become associated with more complex environments (across the spectrum of conflict), there have arisen a correspondingly larger number of counterexamples to such a characterization. Army doctrine has started to bridge the gap between these environments as OOTW scenarios have gained in popularity and operation tempo. Now referred to as stability operations and support operations, these types of missions have clasped hands to commingle those threat concepts traditionally held in one hand as exclusively garrison, or in the other hand, as exclusively tactical. For example, operational doctrine recognizes that commanders executing stability operations or support operations must contend with traditional crimes (drug trafficking, gun running, black marketing, and even rape and robbery) as a threat to mission success. At the other end, administrative threat programs have become increasingly aware of the threats capable of imposing asymmetric effects in the domestic and garrison environments.

The distinction between operational and administrative literature, rather, provides a way of examining threat literature trends based on their doctrinal intent: the intent of one is to explain threat as it relates to operations, while the latter prescribes everyday administrative measures relating to threat. Another way of looking at this distinction is by how sources are naturally grouped. Under the current trend of consolidating Army doctrine (e.g., ST 3-0, the draft of FM 3-0, includes several former FMs or some regulations under draft are consolidating several other regulations), the operational doctrine might include those operational sources that may be naturally grouped together, and vice administrative.

Although the distinction between operational and administrative literature may touch on semantics, it has some important considerations when researching the question of threat. As discussed in the analysis of Army threat doctrine in chapter 4, this distinction is important in recognizing and understanding the effects of a recent trend in Army doctrine to merge these two separate classifications. Where in the past, certainly prior to the publication of FM 100-5 *Operations*, operational doctrine primarily focused on one enemy or opposing forces, it has more recently been forced to consider a much larger array of threats. To accommodate these forces of change, operational doctrine has seemingly reached into the *administrative* inventory to develop or support those changes with respect to threat. This compounded an existing problem. Where Army doctrine has probably always had too many administrative programs and concepts, they were at least separate and distinct. If the Army could have differentiated between the number of threat ingredients before, this recent trend has now stirred the pot.

With the exception of opposing forces at the high end of the spectrum of conflict, this recent trend in Army doctrine seems to embrace all threats in somewhat of a catchall fashion. At the lower end of the spectrum, doctrine recommends planning and preparation against a vast possibility of threats. This has both theoretical and real-world implications. Theoretical implications include redundant, generalized, and unstructured threat doctrine. Instead of creating a useful model, such as that used for calculating combat power relative to the well-defined threat from an opposing force, commanders and staffs must now contend with a shapeless variety of threats opposing Army interests. Hence, while planning operations, commanders and staffs must plan contingencies against a menu of threat definitions or descriptions from a variety of sources that are often open for interpretation, confusing, or general in nature.

The real-world implications of this trend are that commanders and staffs must synthesize a complex picture of threat and decipher from it, something meaningful within the specific context of their own environment. Also, without standard threat doctrine, domestic threat intelligence must be conducted in a piecemeal fashion. Intelligence priorities from higher headquarters can become skewed by local considerations. An emphasis placed on collecting against one type of threat group by a request from higher headquarters may be misdirected by the more immediate threats opposing installation interests. Under these conditions, intelligence requests targeting only serious installation threats may receive reports on a variety of threats, including drug traffickers, graffitist, gangs, even traffic offenders. Consequently, reports that are generated as a result of local analyses often report crimes or threats as more serious than they are in reality or they

request more counterthreat assets or dollars than the threat warrants, or they suffer from inaccuracies such as confusing different threat groups.

Joint doctrine, however, seems to have "cherry picked" its choice of threats for consideration and development. Like Army doctrine, it too is concerned with the threat presented by asymmetric effects. Joint doctrine, however, fills its "basket" from that portion of the threat spectrum alone. This has allowed it to selectively field more specific doctrine that combines both administrative and operational threat doctrine under the same jacket. For instance, JP 3-0.7.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, rolls up antiterrorism as an aspect of both administrative and operational doctrine. Although it has some of the requirements of a program, it develops the subject as an operational consideration. Other publications that focus on this type of asymmetric threat include:

JP 3-07, *Joint Doctrine for Military Operation Other Than War*

JP 3-07.7, *Joint Tactics, Techniques, and Procedures for Domestic Support Operations*

JP 3-10.1, *Joint Tactics, Technique, and Procedures for Base Defense*

JP 3-54, *Joint Doctrine for Operations Security*

Perhaps the most readily visible trend in joint doctrine is its focus on terrorism as the primary threat in a domestic environment, and certainly emphasized as a consideration for threats during any operations across the spectrum of conflict. This trend has probably done more to raise the visibility of terrorism and terrorism-related programs, literature, and funding among the constituent services. Along with literature on weapons of mass destruction, which is considered a tactic of terrorists, terrorism has

become the buzzword for installation defense planning and resourcing. It has catalyzed new or highlighted existing sources of literature concerning installation defense, including *The Installation Commanders' Antiterrorism Handbook,* the *Antiterrorism Force Protection Installation Planning Template*; and Training Circular *19-16 Countering Terrorism on US Army Installations*.

Other trends in joint threat doctrine include a trend toward specificity. As discussed in chapter 4, this trend has advantages and disadvantages. Suffice it to say, for now, that while joint doctrine may have developed a more sophisticated methodology for determining threat, it may not be general enough to accommodate all viable threats.

Legal Doctrine and Regulations

Without question, the most important literature category related to DTIM is that body of literature that governs its operations. This literature includes those laws affecting military support to civilian authorities and DoD, Army regulations, and, in a few cases, joint and Army doctrine. Unfortunately, with respect to DTIM operation, most literature does not focus so much on what the Army can do, as it does on what the Army cannot do.

As discussed in chapter 1, there has been a traditional separation between military authority and civil operations stemming from the late eighteenth century that passed into US laws with the Posse Comitatus Act of 1878. This act prohibits the use of the military to execute civil laws except under circumstances expressly authorized by the Constitution or an act of Congress. While its primary purpose is to prohibit the use of the military to directly assist in civil law enforcement activities, it also inhibits other types of military operations within the civil sector and, more specifically, those against US citizens. The

source of this prohibition stems from and is passed forward to the military by the following US codes:

1. 18 USCA 1385: Ascribes the Posse Comitatus Act

2. 10 USCA 375: Requires the Secretary of Defense to "prescribe regulations" limiting military involvement in conjunction with civil officials[4]

Court interpretation has supported the separation between military and civil authority. Generally, it has held that military support short of actual search, seizure, arrest, or similar confrontation with civilians is not a violation of the Posse Comitatus Act. Examples of permitted support include traffic direction and the provision of information, equipment, and facilities. Court interpretation, however, continues to evolve in appellate cases where the defense has alleged violations of the Posse Comitatus Act by military-civil law enforcement practices. Although insightful, such changes are complicated and subtle, but may provide evidence of a new trend whereby the courts are finding or affirming increasing latitude for activities pursuant to military purpose doctrine. The challenge, however, may center on the problems associated with court documentation: Courts only document "case findings" under the appellate system, which may preclude important findings with respect to either Posse Comitatus or military purpose doctrine.

All DoD and Army regulations governing either military support to civil authorities or military operations in the domestic environment implement the Posse Comitatus Act. These regulations can be divided into two categories: those generally governing military support to civil authorities and those specifically governing military operations in the domestic environment or against US citizens. An example of

regulations from the former category is provided below, followed by an example from the latter category:

Military Support to Civil Authorities

DoD Directive 5525.5, *Cooperation with Civilian Law Enforcement Officials*, 15 January 1986

DoD Directive 3025.1, *Military Support to Civil Authorities*, no date

DoD Directive 3025.12, *Military Assistance for Civil Disturbances*, 4 February 1994

DA Regulation 500-51, *Support to Civilian Law Enforcement*, 1 August 1983

Military Operations in the Domestic Environment or Against US Citizens

Executive Order 12333, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982.

DoD Directive 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*, no date

DoD Regulation 5200.8, *Security of Military Installations*, 25 April 1991

Army Regulation 381-10, *US Army Intelligence Activities*, 1 August 84

Despite legal restrictions of Posse Comitatus, laws, court findings, and regulations also provide some exceptions for military support to civil authorities, as well as military operations in the domestic environment. As discussed earlier, exceptions, such as the military purpose doctrine and the inherent authority and responsibility of the installation commander to maintain law and order and protect the inhabitants of the installation, provide some latitude for conducting military law-enforcement operations under similarly prohibitive conditions. Trends with respect to these exceptions are discussed in chapter 4, with some conclusions and recommendations for negotiating the complications and liabilities of these exceptions provided in chapter 5.

Perhaps the Army's expertise in this area lies with USACIDC. As provided by the following regulations, this organization is the Army's only investigative body with authority to conduct investigations off the installation:

> Special agents are authorized to apprehend any person subject to the UCMJ, regardless of location, if there is probable cause to believe that a person has committed a criminal offense.[5]

> Military Police Investigators, who are not members of USCIDC, have no investigative jurisdiction over criminal incidents occurring off the installation.[6]

This flexibility to conduct investigations off the installation requires USACIDC to specialize in the complex law enforcement tasks associated with civil jurisdictions. It must routinely balance the consequences associated with a failure to anticipate domestic threat from off post sources with the legal liabilities associated with Posse Comitatus. Although not an enviable position, USACIDC has continued to improve and refine its doctrine with respect to successfully achieving both ends. In fact in 2000, it published Operations Memorandum 002-00, which was written to clarify several aspects of force protection and DTIM operations. This document provides some fundamental guidance with respect to threat analysis and the legalese associated with DTIM operations.

---

[1]William S. Cohen, "Preparing for a Grave New World," *Washington Post*, 26 July 1999, A19.

[2]Department of the Army, US Army Criminal Investigation Command, Operations Memorandum 002-00, *Force Protection Initiatives and Domestic Threat Intelligence Management (DTIM)* (Fort Belvoir, VA: USACIDC, February 2000).

[3]The White House, *A National Security Strategy for a New Century* (Washington, DC: The White House, December 1999), 15.

[4]Title 10, USC, 375.

[5]US Department of the Army, Regulation 195-2 *Criminal Investigation Activities* (Fort Belvoir, VA: USACIDC, October 1985), 3-21.

[6]US Department of the Army, Regulation 190-30, *Military Police Investigations* (Washington, DC: Department of the Army, June 1978), 4-2.

CHAPTER 3

RESEARCH METHODOLOGY

> The security environment is further complicated by challenges that transcend national borders and threaten our national interests . . . . Complicating the situation is the continued blurring of the distinction between terrorist groups, factions in ethnic conflicts, insurgent movements, international criminals, and drug cartels.[1]
>
> USACGSC, *National Military Strategy*

Introduction

This chapter outlines the methodology used to conduct this study of the Army processes--and the joint processes as they apply to the Army--for conducting DTIM. It explains the method for analyzing current literature with respect to three questions: (1) "How does the Army determine the threat?" (2) "What are the legal parameters for conducting threat intelligence?" and (3) "How do the first two questions affect current processes for conducting DTIM?" This chapter also outlines how current DoD, joint, and Army doctrine, regulations, policy, and guidance will be used to provide the foundation for some proposed answers to these questions in the form of chapter 4 models and chapter 5 conclusions. Finally, it demonstrates how the latest USACIDC experience and work in this area can be applied to improve or, at least, refine DTIM processes.

Description of the Study

This study determines the status of the Army's DTIM operations with respect to the current understanding of domestic threat and the legal implications of related intelligence processes. It addresses the current position of joint and Army doctrine to evaluate its strengths and weaknesses. Using this evaluation as a starting point, it discusses some of the latest developments in conducting DTIM from the perspective of

USACIDC and other parallel research. Finally, it leverages past DTIM experience with some new ideas to design new models for improving or refining DTIM operations. Although these models are not presented as definitive answers to the aforementioned questions, they should provide a more formal and structured methodology for future conduct and analysis or at a minimum provide insight for future training, implementation, and research.

A review and an analysis of how the Army perceives a domestic threat provided the cornerstone for this study and the subsequent development of a model for determining domestic threats against installation. Laying the foundation of "what constitutes a threat" was essential to the subsequent review and analysis of "how to conduct DTIM." Research in this area focused on Army guidance provided by numerous field manuals to ascertain how it defines or describes the threat toward Army interests, as well as a review of current threat-related programs (e.g., force protection, physical security, etc.). With the exception of a bona fide *opposing force* during war or other operations at the higher end of the spectrum of conflict, threat in both domestic and operations other than OOTW scenarios (soon to be published as stability operations and support operations in FM 3-0) were considered.[2] During this review, both strengths and weaknesses in Army doctrine were evaluated.

Following the analysis of Army doctrine, the evaluation moves into the joint arena to review the latest momentum in counterthreat guidance. Contrary to the Army's more general view of threat, this review of joint doctrine points to a much more specific picture. It focuses almost exclusively on terrorism as a threat. This specificity provides some additional avenues for analysis and discussion. Because it is more focused, for

instance it offers additional details for profiling threats and, incidentally, a much more sophisticated methodology for gauging their effects.

The juxtaposition of Army and joint doctrine provides a nice counterbalance for determining gaps in current doctrine, while highlighting a potentially more viable approach for determining threat. As discussed in chapter 2, this area was developed and published in USACIDC's *Operations Memorandum 002-00* in February 2000. Here, USACIDC's threat methodology is reviewed and discussed as a compromise between threat descriptions that are either too general or too specific, and, based on the earlier analysis of threat doctrine, evaluated against a backdrop of lessons learned.

This provides a jumping-off point for discussing the development of a new threat model for determining threats against the Army's domestic installations. The advantages and disadvantages of this new threat model are discussed against those of current doctrine. This threat model is also discussed within the context of the next question concerning the legal parameters of performing DTIM operations and, finally, it is reviewed with respect to conducting current DTIM operations.

The next portion of this study encompasses a review and analysis of the legal implications of conducting DTIM. The analysis in this area, springboards off of the discussion in chapter 1, "Problem Background," concerning the legal parameters involved in conducting DTIM within US boundaries. It includes a discussion of USACIDC's legal guidance for conducting DTIM, which was published as a part of *Operations Memorandum 002-00*. Although this guidance was certainly indicative of such factors as the complex nature of the legal implications of domestic military operations and the underdeveloped nature of domestic intelligence doctrine, it presents a

problematic scenario for gauging the liability involved in this area. The discussion also includes an analysis of the shortcomings of this example of traditional guidance and provides some insights based on practical experience and analytical conclusions.

From this traditional understanding, the study expands to include a discussion of the on-going evolution within the legal environment, based on the court appellate system. It includes research using the Lexus-Nexus search-engine to navigate the largest legal database in the US to sample cases involving DTIM and DTIM-related issues. The following phrases represent an example of some of the selections used to prompt this search:

Criminal Intelligence
Domestic Terrorism
Domestic Threat
Military Intelligence
Military Law Enforcement
Military Purpose Doctrine
Posse Comitatus Act

While findings, by no means, include all relevant cases, those analyzed and discussed may generally represent certain aspects or trends in these evolving legal criteria. Samples discussed, too, will demonstrate the methodology for this analysis, may provide a basis for other interpretations, or may include findings that directly or indirectly impact traditional interpretations. Examples promoting change must also be discussed within the context of DTIM operations. What are the second and third order effects of fundamental changes within the appellate system? This aspect will be developed using several examples of such potential changes and effects.

Finally, this section proposes a new model for determining the military nexus as discussed in chapter 1. This new model suggests a systematic process for organizing and

prioritizing elements essential to determining a military nexus. It also provides metrics for evaluating the potential legal liability involved with domestic operations.

Research Analysis

The research analysis for answering the primary and secondary questions will require some unorthodox procedures. Although the methodology will include elements from several research approaches, such as descriptive and comparative analysis, it will primarily leverage personal experience to analyze and to assess current DTIM processes and will develop and discuss some new models for determining threat and legal liabilities.

The use of models to answer the primary and secondary questions may provide the best medium for outlining the conclusions. Models or templates can be used to demonstrate the complex nature of the criteria involved in DTIM (e.g., legal criteria, threat criteria, and areas of application). Models will also assist with formulating the interrelationships between concepts and conclusions and ultimately, may be a more effective way to outline conclusions, discuss recommendations, and suggest future research in chapter 5.

Conclusion of the Study

This study concludes with the proposal of two models that address two of the most essential processes within DTIM: determining threat and legally managing domestic intelligence. Collectively, these two models, in and of themselves, answer the primary and first three secondary questions. The last secondary question, How will DTIM processes parallel criminal intelligence processes in a tactical environment? is discussed as a theoretical conclusion and an area for further consideration in chapter 5.

Testing the validity and reliability of the proposed models for determining threat and the legal liability involved in DTIM is well beyond the scope of this thesis. Time constraints and the Herculean task of collecting, collating, and organizing criminal data or using criminal data to develop realistic crime scenarios for testing the models would surpass the most generous time constraints. As time and resources allow, however, these models may (as discussed in chapter 5) provide new and fertile ground for the germination of future research. Preliminary validation relied upon the analysis of the strengths and weaknesses of current doctrine, personal experience, and a common sense approach.

---

[1]Department of the Army, US Army Command and General Staff College, *National Military Strategy* (Fort Leavenworth, KS: USACGSC, August 2000), 7.

[2]Department of the Army, US Army Command and General Staff College, ST 3-0, *Operations* (Fort Leavenworth, KS: USACGSC, October 2000), chapters 10 and 11.

CHAPTER 4

RESEARCH ANALYSIS AND RESULTS

> This country swarms with vile outrageous men/That live by rapine and by lawless spoil[1]
>
> Christopher Marlowe, *Tamburlaine the Great*

Introduction

This chapter reviews and analyzes three critical areas affecting DTIM operations. As outlined in chapter 1, it is comprised of three sections: Determining the Threat; Defining Legal Parameters for Conducting DTIM; and Conducting DTIM Operations. The first section provides an analysis of problems confronting the Army's current view of domestic threat with regard to terminology and program redundancy. It traces progress in joint and Army antiterrorism doctrine, and from an analysis of antiterrorism TTP, provides some insight into USACIDC's latest domestic threat model, followed by some proposed changes in the form of a new threat model. The next section reviews the legal implications affecting domestic threat intelligence processes, and USACIDC's latest guidance, and from this analysis presents and discusses a new model for legally managing DTIM processes. Finally, the last section discusses the implications of the first two sections on current DTIM operations. It integrates conclusions from the previous sections to offer some answers to the primary question, How should Army law enforcement legally conduct DTIM and apply it to assess the domestic threat against continental US installations?

Section I: An Analysis of Domestic Threat Doctrine

Domestic threat intelligence must be inextricably tied to an accepted, common understanding of domestic threat. Without a common definition of domestic threat, development of subsequent doctrine will continue to be diffused among different programs, operations, and services. Conceptual standardization is also important because it is this shared understanding of threat that provides the foundation for managing domestic threat intelligence. At its most fundamental level, it should explain what constitutes a threat, and at more sophisticated levels it should provide threat classifications, methodology for determining threat priorities, and procedures for threat mitigation. Any success at more sophisticated levels, however, begins with success at the lowest level: formulation of and agreement on a common understanding of what constitutes domestic threat.

This section discusses the issues concerning the development of current domestic threat doctrine. It begins by stressing the importance of the link between defining domestic threats and conducting DTIM. It explores some of the unanswered challenges in establishing this link because of confusion created by a lack of information in a comparably underdeveloped field, and by too many subtle--but distracting--variations in definitions and terminology. Development of a common threat doctrine has also been confounded by inconsistencies in defining domestic threat across other emerging areas including programs (e.g., force protection, security, antiterrorism, etc.) and operations (e.g., domestic, peace, humanitarian, etc.).

Additionally, an analysis of the challenges affecting DTIM operations would not be complete without some discussion concerning the military's current focus on

terrorism. By all indications, terrorism is considered the most probable threat in the domestic environment, while still presenting a formidable threat in the full range of "stability operation and support operation" scenarios.[2] Such emphasis has proven to be a double edged sword. On one side, it has sliced through the inertia of what was, prior to the last decade, a rather stagnant field. Work in the area of terrorism has fostered interagency, interservice, and international collaboration, catalyzed resources, and provided insight in determining, measuring and countering such activities. This early impetus offers more than its intended value; antiterrorism doctrine offers insight and ideas beyond countering a single threat that may be applied to a broader range of threats. Cutting the other way, however, improvements in antiterrorism doctrine have been at the expense of countering other potentially viable threats in the domestic environment. Although just one of several components of the force protection program, antiterrorism has--as probably most field experts will agree--garnered the lion's share of funding, resourcing, and publications. These twin implications of a threat policy leaning toward terrorism are further developed in subsequent paragraphs, and reconciliation between its successes and shortcomings offered in the form of a new model.

Linking the Threat and DTIM

Understanding the potential threats confronting domestic installations (e.g., terrorists, drug traffickers, extremist, etc.) is paramount to conducting DTIM operations. Like any other form of military interdiction, a clear picture of the threats' intent, capabilities, history, etc. is requisite to planning countermeasures to deter, detect, detain, or defeat them. The Army's opposing forces doctrine, for instance, provides a good example of a well-developed linkage between the threat (in this case, the enemy) and the

intelligence processes essential to countering it. This linkage allows planners to project themselves into the enemy's decision cycle to plan actions, predict reactions, and prepare for counteractions. By understanding the enemy, his history, intent, capabilities, etc., planners can use the military decision making process (MDMP) to develop both the enemy's "most likely" and "most dangerous" courses of action," and develop plans and contingencies to counter them. The MDMP process also allows planners to focus their intelligence assets to confirm or deny enemy actions and either execute the plan, initiate a contingency, or reinitiate the planning process.

Defining what constitutes a threat, then, is the first step in managing domestic threat intelligence. (Generally an antagonist is referred to as *threat* rather than *enemy* in domestic and OOTW scenarios.) It assists force protection and security managers, law enforcement, and intelligence agencies to focus their collection efforts. As discussed in chapter 1, identifying the threat allows commanders to appropriately plan defenses, allocate resources, and tailor counter-threat responses. Ideally, this identification process should occur at two levels. The first level should be established in doctrine, SOP or as a part of designated threat TTP. This level represents the body of knowledge concerning domestic threat. It should encompass the types of threat groups, their activities, and their potential effect on the installation and force protection objects in the domestic environment.

The second level occurs at installation level--with the exception of those occasions directed by higher guidance--as a part of installation security and force protection activities. Here, commanders and staffs first develop the local threat scenario based on solid doctrinal concepts of domestic threat, and then tailor it to the particular

aspects associated with their security environment. This second-level refinement is shaped by local domestic threat intelligence and takes into account installation defenses, target values and other local variables. Installation commanders, familiar with doctrinal concepts, work through the staff process to determine the most likely and most dangerous threat scenarios. At this level, they should appreciate how a first-level understanding of threat groups and activities affects second-level processes, and how understanding one allows them to effectively shape the other.

Analysis of Current Threat Doctrine

Defining potential threat in the peacetime domestic environment has not, however, been easy, and efforts over the last decade to establish standard criteria have met with only limited success. Publications designed to develop, expand, or clarify a realistic threat have been marked as much by distractions associated with their own proliferation, as they have by any progress toward integration and standardization. Perhaps more a product of a zealous enthusiasm than a lack of commitment, guidance published in military regulations and field manuals (FM) throughout the 1990s has suffered from what can be described as the "Winchester House" effect, where continuous development has outrun blueprint design. Instead of providing a single integrated definition of threat, doctrine has left the analysis of threat to be extrapolated from the nature and number of programs and concepts designed to counter it. Consequently, programs or concepts are analogous to rooms in the Winchester House; each one adds square footage with little regard for the overall floor plan.

Although this fragmentation should not be overstated--as draft doctrine continues to refine and integrate current publications--it must be considered problematic to

establishing standard threat doctrine. Examples of this fragmentation can be easily provided, but it is much harder to place a finger on the problem, and, harder yet, to summarize. Scanning any number of regulations or FMs concerning the definition of threat, or any topic related to threat, will produce numerous examples of "program cannibalization," where threat programs or concepts literally try to consume each other. They often include--by their very definition--other programs or concepts, or common elements, or even provide many of the same functions or measures to counter threat. A quick review of some common definitions reveals this pattern of similarity:

> Force Protection: security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs . . . . The four components of force protection are: operational security and deception operations; the soldier's health and morale; safety; and the avoidance of fratricide.[3]

The definition of force protection from JP 1-02 does not include the four components. Although force protection includes the four components in FM 100-19, it also integrates *law enforcement operations*, and JP 3-07.2 omits "the four components of force protection."

> Security: (JP1-02) 1. Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or that may, impair its effectiveness. 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 3. With respect to classified matter, it is the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (NATO)--A condition that results from the establishment of measures which protect designated information, materiel, personnel, systems, components, and equipment against hostile persons, acts, or influences.[4]

(FM 100-23 adds a more specific threat to security operations.)

> Security: [n]ever permit hostile factions to acquire an unexpected advantage." In peace operations, security deals with force protection as a dynamic of combat power against virtually any person, element, or hostile group. These could include terrorists, a group opposed to the operation, criminals, and even looters.[5]
>
> Protection: Operational protection also includes…employing operations security (OPSEC)--to include providing physical and personnel security, and conducting deception.[6]

Because of their similarity, these definitions provide several points of redundancy: (1) most of them provide similar counterthreat guidance or services; (2) although disguised by different terminology most of them are comprised of the same components or elements; and (3) most of them counter the same general threats. As to the first point, terminology such as force protection, protection, operational protection, antiterrorism, and security all provide similar guidance for countering threats. Yet a comparison of those definitions outlined above, or even those from other sources, indicates that these definitions vary only slightly from one to another. Essentially, when installations, organizations or persons are conducting security or force protection operations, protecting the force, or practicing protection, they are doing the same thing. Even whether or not one might infer that one term is subordinate to another (e.g., force protection is an element of security, or physical security is an element of force protection, etc.) seems unimportant in light of the relatively small value added.

A second point of redundancy is created as a result of programs or concepts containing many of the same elements or components. These may include operations security, deception operations, physical security, combating terrorism, safety, personal protective services, and soldier health and morale. Core terms such as force protection, security, and protection, for instance, all contain a component of personal security or personal protection and asset loss prevention. Moreover, many of these elements or

components are not only subordinate to a larger catchall program, but may also serve as major stand-alone programs in their own right, governed by their own respective regulations or literature and included as a separate and independent subject in a variety of FMs or regulations. Safety provides an example of both: although it is a component of force protection, it is also covered by its own regulations, as well as included as a separate topic in FM 100-23, *Peace Operations*.[7]

Additionally, even program components or elements may include each other as part of their definition. For instance, although combating terrorism and physical security are both "integrated" as part of force protection, antiterrorism is included as an appendix to the Army Physical Security Regulation AR 190-13. Conversely, JP 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, includes physical security measures and the physical security related measures of building and lock security in several of its appendices.[8] As if this is not enough coverage, regulations may even provide additional "blanket" coverage as a final layer of redundancy. The latest definition of force protection, for example, states that it is a "security program designed to protect . . . through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence . . . and other security programs."[9] To what other security programs is it referring? Are there more?

Finally, another point of redundancy results from the fact that much of the Army's terminology provides guidance against a general, rather than a more specific threat. Because the threat picture is so general, any concept or program countering it tends to be overlapped by others. With perhaps the exception of antiterrorism--and even here, there

is some room for inclusion--any one of the aforementioned counter-threat concepts and programs provide guidance against a broad array of threats including, those mentioned in the definitions above, that contain most everything from terrorism to a group opposed to the operation to criminals and looters to what, presumably, may be simply viewed as any force countered by any one of these many counter-threat programs or concepts. Even the new ST 3-0 skirts this problem, citing the traditional broad array of threat activities "that include terrorism, illegal drug trading, illicit arms and strategic material trafficking, international organized crime, piracy, and deliberate environmental damage."[10] Additionally, "extremism, ethnic disputes, religious rivalries, and human disasters contribute" to the threat problem.[11] In the final analysis, such general threat descriptions are not much more insightful than the catchall definition for security provided in *Operational Terms and Graphics*, which describes things that must be protected against "any hostile acts, persons, or influences."[12]

The advantages of such a general view of threat, of course, are that any or all programs or concepts can easily accommodate it, and, therefore, threats can be addressed by any number of measures provided by any number of programs and resources. Consequently, the local USACIDC office, the provost marshal office, the installation force protection office, the physical security office, or even the safety office may provide their expertise to countering either installation threats or vulnerabilities.

The disadvantage, however, is that such a general view fails to develop a realistic or probable threat picture. Rather than providing a central focus, it diffuses counter-threat guidance and activities across a wide variety of concepts that create layers of redundant programs, systems, and measures with little regard for force or resource

economy, the synergy created through program coordination, or the specifics of the threat.

More importantly, the Army's failure to define threat in any systematic way has generated a field of generalists instead of the kind of specialists required to link intelligence with threat analysis. This idea may be better expressed using a metaphor from the medical field: simply put, if all doctors were generalist (e.g., internal medicine), medicine would probably lack the focus provided by tens of specialists, who offer a greater understanding of specific diseases, who could identify diseases or injuries earlier, and who are more skilled at countering them. In this metaphor, disease pathology can be likened to threat intelligence: the more we specialize on specific diseases or threat groups, the more likely it becomes that medicine can provide early detection, marshal appropriate resources to counter them, and mitigate their effects should they strike.

If the Army is to successfully conduct DTIM operations, it must sort through the confusion created by redundancy in its domestic threat terminology, concepts, and programs. It must consolidate and focus threat doctrine. Because the importance of such doctrine goes beyond an academic exercise in semantics, it has real-world implications. With one hand, each threat-related concept or program initiates the writing of regulations, FMs, and other directives, and with the other hand, directs installation counterthreat plans, implementation, and exercises. Thus, each concept or program mandates command responsibility and staff oversight, directs counter-threat related activity, and expends manpower and resources. Even if every concept or program offered clear, perhaps, even unique guidance for countering threats--whether part of a particular operation, against a particular antagonist, or associated with a particular target--without

improved integration and coordination they present an overwhelming and complex set of requirements.

Moreover, the cumulative effects of such redundancy may have created competing programs that duplicate requirements, confuse counter-threat responsibilities, and/or compete for the same resources. As a result, installation threat management often spends more time and energy coping with program requirements rather than countering installation threats. Instead, threat management must continue to sort through a litany of concepts and programs to develop counterthreat measures defined as much by the number and types of programs, as by any indication of threat.

Focusing on the Terrorist Threat

Recent momentum in the field of force protection and domestic security has increasingly focused on terrorism. This trend has evolved over the last decade from earlier doctrine that focused on a much broader array of dangers confronting force protection objects, including the effects of weather, human exhaustion, operational negligence, and a broad spectrum of antagonists. In addition to antiterrorism, force protection programs focused on law enforcement, safety, physical security, operations security, and information security.

As this trend evolved, it entered an interim period where force protection doctrine became increasingly associated with antiterrorism. Although antiterrorism is an element of force protection, titles of force protection manuals and other literature often included both “force protection” and “antiterrorism,” creating the common abbreviation “FP/AT.” In reality, this placed the emphasis on terrorism as a threat on equal par with all other threats combined. And if perception is reality, many future senior leaders at CGSC

confirm this emphasis. (In fact, an informal survey of 25 colleagues at U.S. Army Command and General Staff College [Class 2000/2001], found that 23 answered "terrorist or terrorism" to the question, "What is the number one threat within U.S. boundaries?" With regard to the other two respondents, one answered, "asymmetric threats" and the other "bombing." Of these latter two, the first describes a larger threat category that includes terrorists, and the second describes a common terrorist tactic.)[13]

Whether or not antiterrorism is a subordinate element of force protection is probably irrelevant. Antiterrorism policy continues to dominate domestic defense planning and execution, supported by a strong field of recent antiterrorism publications and literature, including the *Joint Tactics, Techniques, and Procedures for Antiterrorism*; the *Antiterrorism Reference Library*; and the *Installation Commanders' Antiterrorism Handbook*. Also, publications covering other forms of security and protection usually include more than just a casual reference to terrorism.

This emphasis on terrorism, however, has its advantages. As mentioned earlier, the area concentrating on terrorism has provided some notable exceptions to threat redundancy. For the most part, it offers a program that is focused on a single threat group--terrorists. Catalyzed by domestic threats such as the domestic bombings in New York and Oklahoma, combating terrorism has become a vibrant program, garnering the lion's share of attention, money and resources. In fact, for a majority of the last decade antiterrorism initiatives and measures have competed in the areas of security and budgeting for additional resources, such as "victory over terrorism" (commonly referred to as VTER) funding. Moreover, as joint doctrine has turned its attention to focus more and more on asymmetric threats, antiterrorism has become the centerpiece of its doctrine.

This emphasis on terrorism has provided some important benefits to the field of domestic security. First and foremost, it has heightened U.S. awareness of the dangers of asymmetric threats to the American homeland. It has forced Congress to rethink current laws with respect to the balance between individual freedoms and domestic security. In fact, according to the Navy Times, the Senate passed yet another amendment to the Posse Comitatus Act in 1995 that would "allow the U.S. attorney general to call in the military when terrorists have used or threaten to use chemical or biological weapons. Since 1982, the law has allowed the military to be called in on cases involving nuclear weapons."[14] These changes, with regard to the use of military in support of civil law enforcement, confirm a general willingness to reevaluate traditional values embodied in the constitutional and legal systems, as well as foreshadow a trend toward reevaluating the role of the military for countering domestic threats. Additionally, the focus on terrorism has generated three other essential benefits: (1) it has focused the TTP aspect of threat doctrine, (2) it has marshaled resources for all programs willing to provide antiterrorism measures, and (3) it has generated additional publications.

Expanding Joint Antiterrorism for a New Threat Model

Benefits, notwithstanding, work in the area of combating terrorism may still have some room for improvement. A quick review of the definition for terrorism from JP 3-07.2 provides the basis for the subsequent analysis:

> The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments of societies in the pursuit of goals that are generally political, religious, or ideological. (This term and its definition replaces the existing term and its definition and is approved for inclusion in the next edition of JP 1-02).[15]

This definition has several key elements essential to understanding terrorism as a threat. First, the definition does not so much hinge on what the activity is, as it does on its intent and purpose. While the activity will certainly be unlawful, this would hardly distinguish it from any other type of threat activity. Arguably, all domestic threat activities are unlawful. The intent, however, is decidedly different than that posed by other threats. The intent of terrorism is to create fear. Its purpose is to coerce or intimidate governments in the pursuit of goals that are generally political, religious, or ideological."

This definition of terrorism points out the dangers of an "extreme" type of threat, but is it the only criminal group or type posing a threat against the domestic Army? Joint Pub 3-07.2 offers an answer to this question in its own introduction:

> All acts of violence against the US military are not necessarily terrorist actions (e.g., murder or robbery). The measures contained within this publication provide guidance that will help protect the military unit and service member from these acts of violence as well as those committed by terrorists.[16]

This passage offers two important concessions to the emphasis placed on terrorism. First and most obvious, is its recognition that terrorism neither constitutes all acts of violence against the US military, nor, as a consequence of that fact, can terrorists be considered the only threat group. The second concession to the rather singular emphasis on terrorism is that antiterrorism measures can be applied to protect the military from non-terrorist-related acts of violence, as well as those committed by terrorists. As pointed out in this section, both concessions provide important implications for determining domestic threat.

Within the same passage, this publication develops the idea that not only are there multiple threats, but distinguishing between these types can be rather difficult:

> In peacetime military operations, there is no definitive method of differentiating terrorist acts from other violent crimes because the perpetrator's intent may be the only discriminator. A rule of thumb that can be applied is if the act is obviously related to personal gain (robbery of money or high-value items) or personal motivation (hatred, love, revenge) it is a crime, but probably not terrorist-related. On the other hand, if the acts appear to adversely affect military operations (communications facilities, fuel storage areas) or has a high symbolic value (headquarters, particular individuals), the crime probably has terrorist implications even when no claim is forthcoming.[17]

The focus here is on the importance of determining the threat, but, as it relates to peacetime military operations, it tends to ignore some important implications for threat doctrine. Its most glaring deficiency stems from its failure to recognize that other threat acts (or what it refers to as "violent crimes") will "adversely affect military operations." Almost any threat act, at one level or another, will adversely affect military operations. Drug trafficking, theft of military equipment, gang violence, or a host of other types of threat activities will affect military operations--if for no other reason than the fact that it simply degrades readiness.

While determining the threat intent can be important for planning countermeasures, the relevance of intent is not exclusive to countering the act. In other words, just focusing on threat intent will neither prevent the act in every case, nor necessarily mitigate its effects. Instead, the threat model should accommodate other possible scenarios that may arise as a consequence of other types of threats. First, unlawful acts may have unintended consequences that create a terrorist type incident. A botched bank robber may take a hostage. How would this scenario be substantially different than if the hostage-taker was a terrorist? It would certainly adversely affect the military installation.

A second scenario might be created by other nonterrorist threat groups committing terrorist-like acts without the intent "to inculcate fear; [or commit unlawful acts] intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological." Such acts may be the result of nothing more than "personal motivation." The movie "Die Hard," for example, provides an example of this type of scenario. In the movie, a group of criminals use terrorist tactics as a deception to divert attention from their real purpose--to steal millions in negotiable bonds. Nevertheless, their actions and those of the police and FBI were exactly the same as they might have been if their intent had been that of terrorists. Ironically, the success of their caper actually hinged on the FBI using counter-terrorism tactics to mitigate the situation.

Another very real, but benign example of nonterrorists committing terrorist-like acts is the perpetration of a terrorist hoax, such as leaving a fake package at a strategic location or calling in a bomb threat. Motives for these acts run the gamut from boredom to anger or apathy in workplace to misguided pranks, but in no way constitute terrorism as previously defined. While the initial intent may be harmless, the second and third order effects can create a far more serious problem. Terrorist hoaxes may consume huge quantities of resources, inconvenience large populations, create social stress, or tie up emergency services. Ultimately, such criminal acts could have a domino effect that might lead directly or indirectly to an unintended but similar finale as a terrorist incident, maybe even leading to injury or death. Committing emergency services to a bomb threat, for instance, means that they may not be available for lifesaving interdiction elsewhere.

A third scenario might consider the dynamics of a criminal group. A criminal group (or even a lone perpetrator) may evolve by moving up or down the scale of criminality. As a result, the intent behind their activities may change as they evolve. This is not an uncommon phenomenon. Most law enforcement experts could cite numerous examples of gangs evolving into drug traffickers, exchanging from intent to recruit members to one of profit; or an extremist group such as a militia shifting its intent from nonlethal government protest to acts of terrorism.

Finally, the prevalence of terrorism must be addressed and balanced against resource expenditures. In the last decade 176 people were killed by acts of terrorism in the US. "According to FBI statistics, only 25 terrorist incidents occurred in the United States between 1990 and 1997 (the last year for which figures have been published). The total death toll, however, was the result of only three terrorist incidents."[18] In particular, the bombing of the Alfred P. Murrah Federal Building in Oklahoma City accounts for all but 12 of these deaths. And, as it turns out, none of the victims of any of these incidents were military.

While terrorism perhaps dominates the collective consciousness of Americans--certainly finding an outlet through resourcing priorities of its military--incidents remain comparatively low to those of other countries or even comparatively low as a viable threat in terms of other US domestic incidents causing casualties or deaths. It remains an even lower threat among the Army's ranks, and among those assigned to domestic duty almost nonexistent. This paradox between fear and reality has not gone unnoticed. Bruce Hoffman touches upon this dichotomy between risks and priorities in his article,

Terrorism by Weapons of Mass Destruction: A Reassessment of the Threat. While he is certainly not advocating complacency in the face of such potential danger, he writes:

> Terrorism poses, and will likely continue to pose, a serious threat to Americans and American interests both in this country and overseas. Nonetheless, it is equally clear that there has been a tendency to exaggerate the dimensions of the treat and the strategic impact that terrorist violence has actually wrought. And by overreacting and falling prey to a sense of acute fear and intimidation, we inflate the terrorists' power in ways that are both counterproductive and often divorced from reality.[19]

It is important to understand the implications of such oversights on domestic threat intelligence. If law enforcement is to effectively counter threats, it must accept a model that consists of multiple threats. It must take into consideration all unlawful acts that range across the entire threat spectrum. The advantages of such a model are readily apparent. First, it would naturally accommodate those activities already being conducted by the first line of domestic threat intelligence--law enforcement organizations. Second, it would broaden the scope of intelligence to include all viable threats, and not just focus on the most dangerous. Third, it would recognize the connectivity between crimes. Often intelligence collected on one crime leads to the discovery of others, some of which, present a far more dangerous threat to military installations. Fourth, it would allow law enforcement to leverage known intelligence on an organization that may have changed its intent from a lesser to a more serious threat. Finally, it would place terrorism, albeit still at the top, among a natural order of criminal or threat groups. After all, as recognized by joint doctrine, "terrorist acts are criminal acts" and "in peacetime, terrorist acts are normally punishable only under domestic (local) law."[20]

Essentially then, terrorists represent one of a number of viable threats to military installations. In fact, it represents the *most dangerous scenario*, but not necessarily the

most likely scenarios. (As used here, the term *most dangerous scenario* is substituted for the MDMP term *most dangerous course of action,* to differentiate a threat-action by multiple groups rather than multiple threat-actions by a single group.) This view of threat considers the effects of threat on an installation from a full spectrum of possible threats. Although such a view receives little publicity, it is widely practiced among law enforcement everyday. It represents nothing more than prioritizing crime in the same way that joint doctrine prioritizes terrorist threats. In fact, USACIDC did just that, as published in their operations memorandum 200-02. They divided installation threats into seven threat groups (as outlined in chapter 1) ranging from *terrorism* at the high end, which represents the most dangerous but least prevalent threat, to *unsophisticated crimes* at the low end, which represent the least dangerous but most prevalent threat.

This concept of multiple threat groups is provided in a new threat model at figure 3. The model presents somewhat of a compromise between joint doctrinal processes for conducting threat assessments and USACIDC's view of criminal threat categories. This model provides an improved process in which criminal categories are considered along a threat spectrum from least to most serious, and as defined by USACIDC includes: unsophisticated criminals, drug criminals, gangs/hate groups, extremists (illegal militias), organized criminals, saboteurs, and terrorists, respectively. At each level, criminal activity can be evaluated using a modification of the joint terrorism threat analysis, in which each threat group is analyzed using six factors: existence, capability, intentions, history, targeting, and security environment.[21]

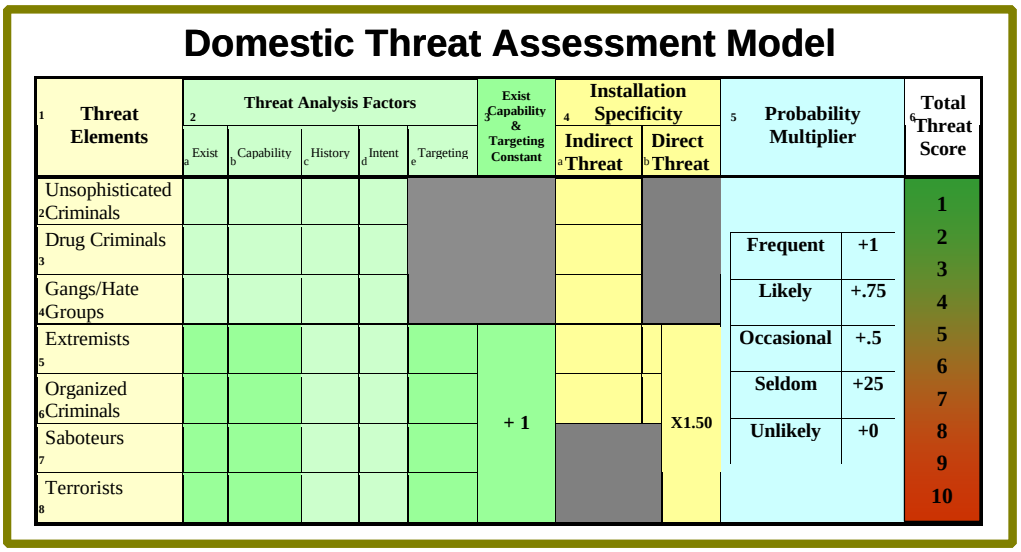

Figure 3. Domestic Threat Assessment Model for Army Installations

In addition to the ordering the threat groups in column 1 from least to most serious, the model also includes additional weightings in columns 3 and 4. These weightings provide a distinction between the potential adverse effects of different threat groups and are annotated by shading out certain boxes to prevent entering a checkmark (i.e., rows 2, 3, and 4 for columns 2e, 3, and 4b; and rows 7and 8 for columns 4a). This is because only the four most serious threat groups (extremists, organized criminals, saboteurs, and terrorists) would generally include the combined threat factors of *existence*, *capability*, and *targeting* and, therefore, are the only ones that can receive the *exist, capability, and targeting constant* for an additional point and the multiplier of *1.5* for demonstrating a direct threat to the installation. Also, the two most serious threat groups (saboteurs and terrorists) by their very nature represent a direct threat to an installation and, therefore, can only receive a checkmark in the box annotating a direct threat, which means that their score is automatically multiplied by 1.5. Similarly, the first

three threat groups (unsophisticated criminals, drug traffickers, and gangs and hate groups) can not, by definition, target an installation and, therefore, cannot receive a point for targeting, nor the point for the *exist, capability, and targeting constant*, nor the direct threat multiplier of 1.5. Otherwise, a threat group receives a point for each block that is checked in columns 1-4, and the appropriate points added from column 5. Consequently, the last four threat groups are the only ones that can receive a total threat score between one and ten points, while the three least serious threats can only receive a score between one and six points.

Total threat scores recognize and provide an important distinction between the frequency, pervasiveness, and effects of threat groups. This distinction goes back to the previous discussion about the most dangerous versus the most likely threat scenarios against an Army installation. While the first three threat groups can affect an installation through the frequency and pervasiveness of their crimes, their effects on the installation are limited by their capability and intent. Gangs, for instance, do not get up in the morning with the intent of targeting and destroying and installation and, certainly, most gangs do not have the capability. That is not to say, however, that they cannot adversely affect an installation. They can and do. They can recruit members from Army population, commit crimes for money and in extreme cases, even target certain persons. If their intent changed for some reason to include more serious affects, then they have probably morphed into a more serious threat group, such as organized criminals or an extremist group.

The four most serious threat groups, in particular the two most serious, can, based on their existence, receive a score from 1-10. The fact that they can receive a low score

attests to the fact that they will probably not represent the most likely threat scenario. On the contrary, installations will more often contend with the impact from the frequency and pervasiveness of the adverse effects from the first three threat groups than they ever will the latter four. A possible score of 10, however, provides consideration for their potential effects in the most dangerous threat scenarios. Limiting the score of 7-10 to the four most dangerous threat groups also takes into account the target perspective. It accounts for the security environment associated with most continental US Army installations.

Section II. Defining Legal Parameters for Conducting DTIM

In addition to a continuous evaluation of threat, the Army faces the rigorous challenge of developing methodology on how to legally manage domestic intelligence operations. As discussed in chapters 1and 2, there are numerous sources that provide information concerning the limitations and liabilities associated with conducting intelligence operations in the domestic environment, but any progress toward developing or expanding *how to* guidance has received far less attention than that focused on developing more passive measures associated with just defining and countering threats. This trend presents the Army with somewhat of a Catch 22 dilemma: on the one hand, installation commanders are expected to proactively counter threats in their areas of interest--often well outside their areas of responsibility (e.g., off the installation)--before threats can adversely affect their installations, but, on the other hand, commanders must avoid the risks associated with civil-military violations that could result from such proactive vigilance.

Factors Limiting DTIM

Despite the competing interests that stem from increased institutional pressure to conduct predictable intelligence against domestic threats on one side, and regulatory guidance and traditions that caution Army law enforcement from such activities on the other, little guidance in support of either side has been forthcoming. Considering extenuating circumstances, however, the lack of any new inquiry or guidance is not altogether surprising. Given the historically low incidence of serious threats to domestic installations, the trade off between risks and rewards seems under-balanced. With only prescience to be gained if a serious threat strike should occur and balanced against the potential risks associated with Posse Comitatus violations, few commanders are willing to conduct DTIM operations in such a low-incident-rate environment. Those who are willing to develop proactive intelligence programs must contend with numerous barriers associated with civil-military law enforcement, including: (1) the complex nature of regulatory and legal guidance in this area, (2) potentially stiff legal penalties for violations of the Posse Comitatus Act ($10,000 or 2 years confinement), (3) potential professional and personal liability resulting from such violations, and (4) the difficulty of implementing change in an Army culture based on tradition and continuity.

Of the barriers to conducting DTIM operations, it is the lack of regulatory and legal guidance that presents the most difficult obstacle. There is little civil-military law enforcement guidance in general, but even less guidance related to the smaller law-enforcement niche of DTIM. Even in those sources that include some reference to intelligence, it is only briefly mentioned it in passing. For instance, FM 100-19, *Domestic Support Operations*, limits its discussion of intelligence operations in reference

to law enforcement activities to a single page. It begins with this general introduction and, although it refers to MI personnel, it is equally applicable to MPs:

> Use of MI personnel during domestic support operations is restricted as a direct result of lessons learned from their improper use in the 1960s [during protest demonstrations]. Consequently, LEA [law enforcement agency] requests for MI personnel or material for counterdrug support must be approved by the Secretary of the Army General Counsel and coordinated through the Department of the Army Office of the Deputy Chief of Staff for Intelligence.[22]

The FM also goes on to describe some of the authorized intelligence activities that may be conducted under disaster assistance operations; again, these operations are currently included under the category of *support operations* in ST 3-0. As such, this guidance can probably be applied to other parallel operations that are characterized by a clearly defined military nexus. Incidentally, this guidance is similar to that published by USACIDC and discussed later in this chapter:

> However, a specific MI mission statement, coordinated through proper authorities, must authorize MI personnel to collect, analyze, and disseminate information. When so authorized, MI personnel may--
>
> 1. Acquire information that may threaten physical security of DoD employees, installations, operations, or official visitors, or that may be needed to protect the safety of any person, that is, force protection.
>
> 2. Analyze and disseminate information to disaster relief personnel and emergency operations centers (EOCs).
>
> 3. Support EOC operations using intelligence preparation-of-the-battlefield (IPB) skills.[23]

Regulatory guidance seems even less insightful. This point is discussed in USACIDC's Operations Memorandum 002-00 as an introduction to its legal appendix, which provided initial legal guidance to USACIDC agents for conducting DTIM operations. As this memorandum points out, not only are the regulations "complicated and unclear," but also their mandate does not even apply to authorized law enforcement

activities. The following passage introduced USACIDC's legal guidance published in 2000:

> The collection, processing, storing and dissemination of information concerning persons and organizations not affiliated with the Department of Defense is governed by DoD Directive 5200.27. This Directive was issued in 1980 and is currently undergoing a rewrite. Its provisions are both complicated and unclear. Unfortunately, the Army regulation which purports to implement DODD 5200.27 is dated 1974, has never been updated and by its own terms does not apply to authorized criminal investigation and law enforcement information gathering activities.[24]

The Legal Problem with Decentralization

With little regulatory precedence and no centralized guidance forthcoming, the Army tends to segregate interpretation and decisions for civil-military guidance by delegating such activities to local installations. As a consequence, legal guidance for conducting DTIM is also relegated to local levels to be deciphered installation by installation. The negative aspect to this approach is that authority and legal experts at higher levels are usually uninformed, or often remain reticent, and guidance, if provided, is usually general and on an issue-as-needed basis. This means that DTIM operations can teeter dangerously in one of two ways: they can either become mired down by local systems and processes, become reactive rather than proactive and, inevitably, become unresponsive to real-time processing; or they can operate in isolation without due legal circumspection and often unrelated to formal threat-focused guidance from the installation commander or other force protection participants. In most cases, however, the DTIM process is given far less attention than that posed in either scenario but, instead, remains on the periphery of security and law enforcement interests.

Decentralizing DTIM creates other challenges related to system inoperability between law enforcement or other intelligence organizations and agencies. The parochial

nature of DTIM often leads to an inability to communicate between installations, between lower and higher organizations, and between internal and external agencies. The use of different terminology or intelligence processes means that different agencies can experience problems while working together. Differences in terminology can affect legal guidance and, as a consequence, create fundamental differences in law enforcement procedures. What might be permissible to one agency can be considered legally intrusive to another. Today, law enforcement procedures may vary not only from installation to installation, but also as a result of turnovers in USACIDC and MP leadership, and lawyers assigned to the installation's Office of the Staff Judge Advocate.

Differences in DTIM terminology, procedures, or legal guidance may also create confusion or redundancy between agency responsibilities and authority during joint investigations, and during other collaborative processes, as well as skewing incident reporting standards. A general lack of legal guidance or opposing legal guidance may complicate procedures or even jeopardize the adjudication process, such as invoking the exclusionary rule or even lead to the dismissal of a case. The lack of confidence from underdeveloped guidance or procedures may also inhibit intelligence dissemination. Because of the legal liabilities associated with DTIM, many military organizations are reluctant to cooperate or share information concerning law enforcement activities. Finally, the decentralization of DTIM can lead to different reporting standards. What might be viewed and reported as a serious threat by one agency may only be viewed and reported as a modest or negligible threat by another.

Analyzing Legal Findings of the Appellate Courts

The rules for conducting DTIM may vary based on the nature of the particular law enforcement activity, as well as on the legal interpretation of the law as it applies to that activity. Law enforcement operations countering drug trafficking and most recently, activities countering terrorism provide perhaps the most visible examples concerning the former, while variations in how military services interpret the Posse Comitatus Act based on appellate court decisions provide ready examples of the latter. Both areas have seen recent change. On one hand the legislature has made several exceptions to the Posse Comitatus Act, while on the other, an improved understanding of the legal implications in the civil-military arena continue to emerge under the interpretations of the appellate courts. The recent legislative changes granting some exceptions to Posse Comitatus are discussed as a part of chapter 5 conclusions regarding the future of civil-military law enforcement activities and, particularly, DTIM. As a practical matter, attention here is focused on the more immediate and applicable changes created by the appellate courts.

Based on appellate court records, individual services may have a different perspective of the legal permissions and exclusions involved in conducting law enforcement based on court holdings in their own respective criminal cases. Unfortunately, research in this area is somewhat limited because only the appellate courts provide case documentation. Nevertheless, the implications of discovery in this area are enormous and well worth the search. Each court holding adds to the growing body of knowledge concerning civil-military law enforcement. Likewise, any precedent that is established provides more information regarding the legal permissions for conducting DTIM. By examining some of the important cases along this line of inquiry, the Army

will be able to refine it guidance for conducting DTIM to better balance the rewards of proactive threat countermeasures with the risks associated with operating in the domestic environment. Although a comprehensive analysis of current legal interpretation is beyond the scope of this research, the following examples from appellate decisions provide one with an appreciation for the diversity, complexity, and insight of interpretations from the appellate courts:

> Purpose of 18 USCS, 1385 is to preclude direct active use of federal troops in aid of execution of civil laws; passive activities of military authorities which incidentally aid civilian law enforcement, however, are not precluded.[25]
>
> Activities which would constitute a passive role which might indirectly aid law enforcement are mere presence of military personnel under orders to report on necessity for military intervention, preparation of contingency plans to be use if military intervention is ordered, advice or recommendations given to civilian law enforcement officers by military personnel on tactics or logistics, presence of military personnel to deliver military material, equipment or supplies, to train local law enforcement officials on proper use and care of such material or equipment, and to maintain such material or equipment, aerial photographic reconnaissance flights and other like activities which would not be unlawful under 18 USC, 1385.[26]

The first two court decisions provide a foundation for the use military purpose doctrine to establish the "military nexus" between the military interests and law enforcement or other civil support activities. Law enforcement activities on and off the installation must have a purpose that is directly tied to military interests. Direct assistance to civilian law enforcement is not permissible, but any assistance rendered as the result of a passive activity or as an unintended consequence of the military purpose is permitted. Also, the military can assist civil law enforcement by providing information, loaning and training personnel on the use of equipment and other materials, provide aerial reconnaissance, and prepare and train on contingency plans to be implemented when called upon by the appropriate authority.

> Defense contractor's challenges to search warrant used to search plant for evidence of conspiracy to defraud government results in neither suppression of evidence nor dismissal of indictment . . . where Air Force's execution of search by its Office of Special Investigations (OSI) because actions of OSI agents were not regulatory, proscriptive or compulsory in nature and even if they were, Inspector General Act (5 USCS appx 3) expressly authorized questioned conduct.[27]
>
> Participation by military personnel in drug investigation for purpose of assisting state and local agencies in investigation of cocaine distribution did not constitute posse where military participation did not pervade activities of civilian officials and did not subject citizenry to regulatory exercise of military power.[28]
>
> There was no willful use of Air Force as posse to execute civilian laws, where, consequent to off-base sting operation, in which airman was arrested during purchase of marijuana, undercover agents searched his civilian wife, took her to air force base, and detained her there, since there was independent military purpose to agents' conduct, and since Posse Comitatus Act is not intended to limit military in prevention of illicit drug transactions by active duty military personnel, whether such conduct occurs on or off military installation.[29]
>
> Collaboration of Marine Corps law enforcement personnel and agents of federal, state and local agencies does not indicate motivation of military personnel to aid in execution of federal law, but rather facts support purpose to control drug distribution involving military personnel; thus, use of military personnel does not constitute Posse Comitatus.[30]

These four cases cite that it was not unlawful for the military to conduct investigations for a military purpose when such activities do not pervade civil law enforcement, nor when participation in such law enforcement (including collaboration with federal, state, or local agencies) does not subject civilians outside of military jurisdiction to military authority. The first case specifically held that military law enforcement was not in violation where its actions were not "regulatory, proscriptive, or compulsory in nature."

Civilians can be detained, however, in cases where the military is conducting an investigation with the purpose of preventing, stopping, or limiting illegal acts that adversely affect military interests. Specifically cited are incidents whereby the military

was assisting civil law enforcement to control drug distribution to military members, whether or not the investigation is conducted on or off the installation.

> Assistance given state police by United States airman in investigation of narcotics cases was not in violation . . . since assistance was not induced, required or ordered by Air Force officials, was of a personal nature and was unrelated to his status as military man.[31]

> National Guardsmen's participation in marijuana arrest in conjunction with Drug Enforcement Administration did not violate Posse Comitatus Act, since they were not part of Army or Air Force but state servicemen, where they had never received orders directing them into federal service, and their command had not been taken away from stat's governor.[32]

These two cases held that the status of military members is relevant to whether or not their involvement is legal. Their status can be determined by their relationship to the service during their participation in civil law enforcement activities. If participation is not induced by the military or in any way compulsory by the nature of the service member's official duties, then participation is probably not in violation of Posse Comitatus. Also, National Guard members are not subject to Posse Comitatus when they are not under the provisions of Title 10. In other words, the National Guard can support civil law enforcement unless activated with current orders for active duty.

> Navy can be given exception to assist Coast Guard in its law enforcement activity . . . there is no violation of 18 USCS, 1385 in its use of Navy destroyer in pursuit, boarding, and seizure of converted fishing vessel suspected of being used for trafficking in marijuana.[33]

Similar to the status of service members, the status of the services themselves, while providing civil-military law enforcement, is relevant to whether or not their involvement is legal. This passage establishes that the Navy, much like Army, is granted certain exceptions for to the Posse Comitatus Act. In this particular case, the Navy may assist the Coast Guard in pursuant to law enforcement. And of course, the "Posse

Comitatus Act does not apply to United States Coast Guard," because it falls under the Department of Transportation.[34]

> Where bulk of government's proof of defendants' guilt in violating federal firearms law's prohibitions against sales to minors and no-residents was product of undercover investigation carried out in large part by several marines at request of Special Investigator of Alcohol, Tobacco and Firearms Division . . . and defendants sought, both to suppress and exclude testimonial evidence produced by Marines' investigation on ground that investigation violated Posse Comitatus, court refuse to reverse conviction.[35]

> Investigator was entitled to qualified immunity from prosecution under Posse Comitatus Act for his inactive role while members of military drug suppression team accidentally shot arrestee during handcuffing, since investigator cannot be said to have violated established law, where "willful use" of Army to execute laws had not been defined adequately by case law.[36]

More intriguing, however, are those cases where the courts may have an indication of a violation of the Posse Comitatus Act or other intrusion, but, nevertheless, rule conservatively in support of the government or military. Several cases have demonstrated that a "violation of 18 USCS, 1385 does not mean that evidence surrendered by military to civilian authorities must be excluded,"[37] just as a "Violation of 18 USCS, 1385 does not automatically mean that evidence obtained as result of violations should be suppressed."[38] To the contrary, in many cases, motions to exclude or suppress evidence have been denied despite indications of unlawful civil-military operations. The last two cases reinforce the seemingly complex and perhaps, whimsical nature of legal interpretation and execution in this area. In one instance, the court refused to reverse the conviction even though the Marines clearly pervaded civil law enforcement operations, first at the request of civil authorities, and second, in a manner that carried out a preponderance of the work. The second case provides evidence that even the courts are

struggling with the lack of precedence from case law in areas pertaining to the Posse Comitatus Act.

Establishing the Military Nexus

The crux of these court holdings and that of the demonstrated process of analyzing, collating, and summarizing their provisions centers on defining the military nexus. Understanding court holdings and how appellate courts interpret the conduct of military law enforcement activities within the narrow exceptions of Posse Comitatus, provides insights into the rationalization between what is legal and what is not. As a bottom line, the Army cannot support civil authority as its primary motive for conducting law enforcement activities unless approved by the appropriate authority. The military nexus, however, can be satisfied "as long as the military pursues the investigation of an offense [or related law enforcement activity] with a view toward establishing facts to sustain a court-martial or to pursue a legitimate military function or purpose, then any incidental investigative benefit to civilian law enforcement officials is immaterial."[39]

Many questions still remain as the appellate courts continue to interpret cases--often characterized by "gray areas" in the law--that establish precedence for civil-military law enforcement operations. Until such time as the courts have defined a sufficient body of information regarding this area of the law, the Army must proceed with caution. It must take the appropriate measures to develop improved systems for both defining the military nexus and training its law enforcement personnel. In the meantime, as a body of legal precedence grows, current court holdings may be used to improve and refine those legal provisions already established by military regulations or other authority, such as DoD Regulation 5525.5, *DoD Cooperation with Civilian Law Enforcement Officials* or

USACIDC's Operations memorandum 002-00. The DoD directive, for instance, establishes the foundation for the military nexus by providing that the following actions are among those permissible:

> 1. Investigations and other actions related to enforcement of the Uniform Code of Military Justice (UCMJ).
>
> 2. Investigations and other actions that are likely to result in administrative proceedings by the Department of Defense, regardless of whether there is a related civil or criminal proceeding.
>
> 3. Investigations and other actions related to the commander's inherent authority to maintain law and order on a military installation of facility.
>
> 4. Protection of classified military information or equipment.
>
> 5. Protection of DOD personnel, DOD equipment, and official guests of the Department of Defense.
>
> 6. Such other actions that are taken primarily for a military or foreign affair's purpose.

Similarly, in response to formalizing DTIM operations in early 2000, the Office of the SJA (OSJA) , Headquarters USACIDC published some basic rules or tenets for gauging the military nexus. These rules were developed to provide USACIDC staff and agents with some basic guidelines for determining the legal parameters of conducting DTIM operations. The guidelines were the product of a joint effort between the OSJA and the criminal intelligence directorate and were developed by creating and analyzing a series of scenarios to establish some basic guidelines for determining the military nexus. Each scenario was consciously written to present some of the more complex legal "gray areas" involved in conducting DTIM operations. The legal staff analyzed each scenario to determine the legal parameters for conducting DTIM operations for each specific case, with the intent of sifting through their conclusions for some common tenets that could be

generalized to other DTIM situations. The following seven bright line rules were developed, approved, and published as an appendix to Operations Memorandum 002-00.

> 1. You can always assess whether you can collect, process, store or disseminate information about non-DOD affiliated persons or organizations. (Establishes the premise that intelligence personnel may analyze, but at this point, leave open the question of how.)
>
> 2. You may always report information to other law enforcement organizations if there is evidence of a threat to life or property or a violation of law, even if you are not authorized to collect the information involved. (Establishes operations at the other end of the spectrum that regardless of outcome, dissemination may occur.)
>
> 3. You may collect information on non-DOD affiliated persons or organizations if you have credible information that they are involved in criminal activity on a military installation.
>
> 4. You may collect information on non-DOD affiliated persons or organizations if you have credible information they are committing drug offenses with active duty personnel off a military installation.
>
> 5. You may collect information on non-DOD affiliated persons or organizations if you a have credible information they are committing criminal acts that constitute a clear threat to DOD property of a direct threat to persons on a military installation.
>
> 6. Decisions on collection, retention and dissemination are extremely facts sensitive…consult your USACIDC legal advisor at the beginning and whenever the facts change.
>
> 7. Do [not]…
>
> a. Collect information about how people vote, their political party affiliation, what organizations they belong to, or how they exercise their constitutional rights.
>
> b. Covertly or deceptively penetrate a civilian organization. [40]:

Both sets of permissible activities provide examples of important guidance for determining the military nexus, but they may lack the systematic approach, method, or process necessary to effectively train law enforcement personnel. Although certainly

prescriptive, lists of permissible activities teach law enforcement persons how to think about, develop, and gauge the military nexus? Do such lists even contain all of the essential variables for establishing the military nexus? Prescriptive measures, for instance, can become confusing in more complex scenarios. Could we conduct domestic threat intelligence against a dangerous criminal upon request by civil authorities? Based strictly on those activities listed as permissible, the answer is probably a resounding "No." However, what if civil law enforcement requested help in locating a violent and extremely dangerous suspect lurking somewhere just off post. Would either of the lists previously discussed provide insight in determining additional variables relevant and essential to defining the military nexus, such as location of perpetrator, threat that he poses to the military community, his current activities, the fact that he is good friends with a soldier on post, or other real-world, every day variations to what otherwise might seem a simple scenario.

Perhaps more importantly, would such prescriptive measures that provide examples of what to do, rather than how to think, allow a forum for growth and change? In this regard, the lesson from the appellate courts is powerful. Determining the military nexus is often a complex process with room for interpretation, change, and growth. A more flexible model for analyzing the wide range of "gray area" scenarios may help law enforcement determine additional variables associated with determining the military nexus and, ultimately, improve the real-time detection of domestic threats. At the least, it will assist law enforcement organizations in discussing the appropriate questions concerning civil-military law enforcement. It will, undoubtedly, generate more questions and hopefully, more answers.

The model at figure 4 provides one such method that might help law enforcement personnel determine the military nexus or its absence, as well as provide a system of metrics to help gauge the legal liabilities associated with conducting DTIM in any particular situation. While certainly not all inclusive, this model provides a forum that could assist law enforcement to accomplish the following five functions:

1. It provides a systematic process for determining the military nexus by helping to identify and articulate legal gray areas.

2. It creates a standard platform for training personnel that might improve the accuracy and consistency of performance in executing laws associated with DTIM operations. Like risk management, it also generates a document for discussing the mitigation process.

3. It provides a worksheet that highlights the relationship between the military nexus and the intelligence process, with respect to the subsequent DTIM activities of either disseminating or storing intelligence.

4. It provides a system of metrics to help gauge the legal liability associated with conducting DTIM for any particular situation.

5. It provides an academic model to capture change with respect to laws and the subsequent interpretation of those laws. In other words, it provides an active link between the legal and regulatory statutes and any subsequent change to those mandates.

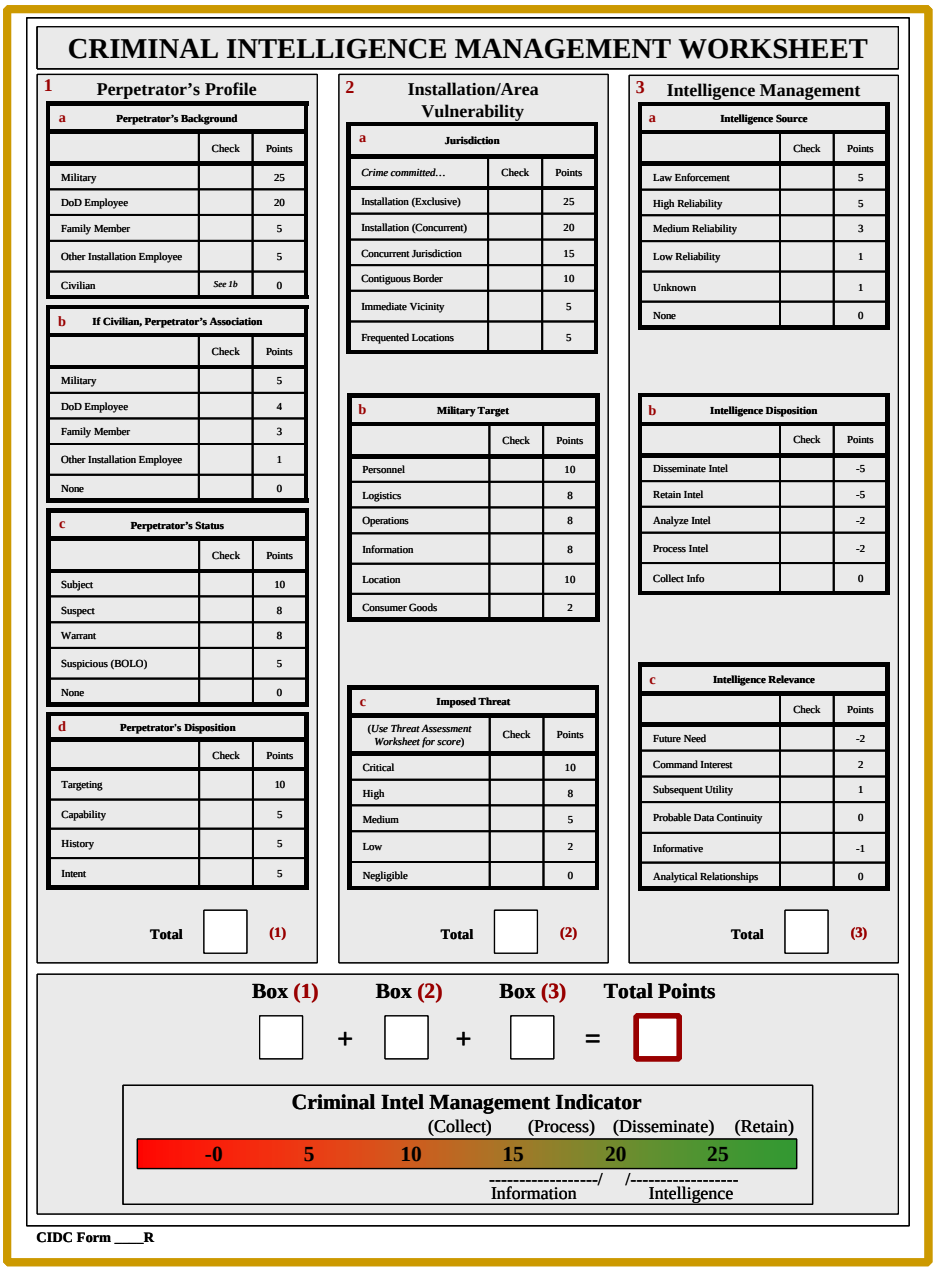

Figure 4. DTIM Legal Assessment Model

The model is comprised of three columns, labeled: *perpetrator profile*, i*nstallation vulnerability*, and *intelligence management*. Each column consists of several variables that represent a set of conditions that are prioritized and given a corresponding

number in accordance with their respective value. Each value is used to determine the link between that particular variable and determining the military nexus or risks associated with conducting DTIM. The first two columns are used to assist--in conjunction with the lists of permissible activities--with determining the military nexus, while the last column is used to assist in determining the liability of conducting DTIM processes, including collecting, processing, disseminating, and retaining.

For example, under the *perpetrator profile* column, the variable of *perpetrator's background* is broken down into five conditions, each ranked in an order based on its value for determining the military nexus. A perpetrator that is military, for instance, has a higher value (25) associated with determining the military nexus then does the civilian, which excluding all other variables, would offer no value for determining the military nexus. Certainly this meets the legal test established in DoD Regulation 5525.5, which grants authority over a soldier under the first of those actions listed as permissible, but nowhere stipulates, excluding all other variables, authority over civilians.

With the exception of the variable of *imposed threat* at the bottom of the second column, all other variables in the first two columns are calculated and justified the same as the example of the *perpetrator's background* variable. The *imposed threat* variable receives its rating based on the threat score from the threat model presented at figure 3. Ranking and scoring for this variable is based on the principle that as the threat increases so too does the permissibility of those actions that might be considered necessary, under the installation commander's inherent authority and responsibility, to protect the installation.

The final column (*intelligence management*) recognizes the range of liabilities associated with conducting the DTIM process. In addition to determining the military nexus, this column captures what military law enforcement personnel plan to do with the information or intelligence. This is an important consideration because each activity from collecting to disseminating or retention may have a different degree of liability associated with it. Collecting information, for instance, may have relatively little liability associated with it, whereas retention of intelligence in a database may generate far more liability, especially if there is no plan or system for purging the data when it is no longer associated with a military nexus. Depending on the conditions of the variables selected, points may be assessed that require a higher score in the first and second columns to offset the higher liabilities in the third column. In other words, there is a direct positive correlation between intelligence disposition and defining the military nexus: the higher the liability associated with its disposition, the higher the threshold for establishing the military nexus.

The points for each column are then added and annotated at the bottom. These points are then added together to come up with a total value for the DTIM worksheet. The total value can then be referenced against the criminal intelligence management indicator scale at the bottom of the worksheet. This indicator ranks liability of a scale from 1-25. Those ratings that fall along the "red" portion or below 15 probably require a stronger military nexus before conducting any law enforcement or DTIM activities. Although all worksheet results should be checked with the installation legal advisor, those rating that fall along the green portion or above 15 on the scale are probably indicative of a well-defined military nexus. This model, however useful, must be used

with caution. It is intended only as a tool to generate and improve discussion and training techniques for conducting DTIM. Its results are not conclusive. As discussed in chapter 5, this model has not received extensive and independent testing. It may require improvements, such as additional variables, changes in assigned point values, or further clarifications.

Section III. Integrating Figures 3 and 4 into the DTIM Proces

Integrating the models at figures 4 and 5 into the DTIM process can be demonstrated both quickly and easily by using the DTIM Model from the USACIDC's Operations Memorandum 002-00. This model at figure 5 depicts the DTIM process as a cycle comprised of four phases: *Intelligence Collection*; *Threat and Vulnerability Assessment*; *Crisis Management*; and *Analysis and Deterrence*. Each phase of the model is associated with installation law enforcement and force protection requirements. These requirements include developing an intelligence network and conducting liaison activities in phase I; providing force protection services in phase II; responding to and mitigating crises in phase III; and investigating, reporting, and capturing lessons learned in phase IV. Each phase is an integral part of the entire DTIM process and, therefore, the requirements in one phase are related to activities in each of the other phases. Although the model demonstrates DTIM as a sequential process, it may actually begin at any phase and continue to the next phase or skip to any other phase. Similarly, the model demonstrates the relationship between the DTIM process and installation THREATCONs that may be upgraded at any point, but THREATCON C and D would generally be associated with phases II and III, respectively.

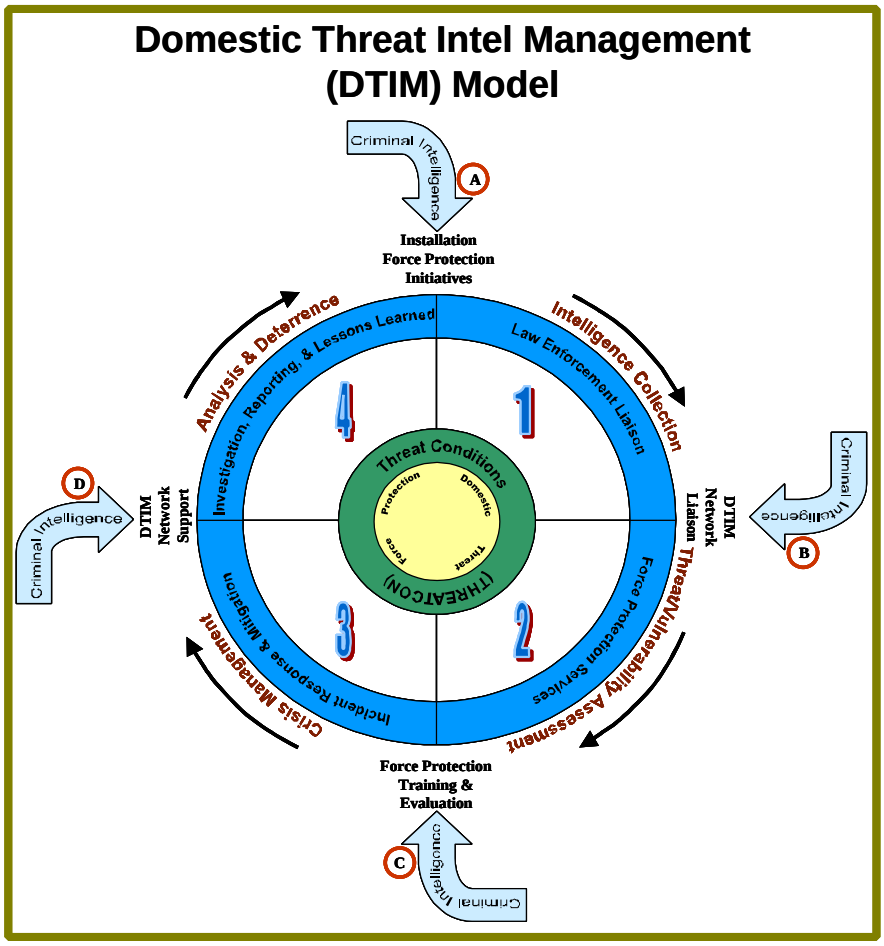

Figure 5. DTIM Model, USACIDC Operations Memorandum 002-00

The activities associated with the threat and legal models in figures 4 and 5 generally occur during phase I activities in preparation for providing force protections services in phase II. These services include providing law enforcement, physical security or other force protection threat and vulnerability assessments (e.g., antiterrorism vulnerability assessment, extremist criminal activity threat assessment, economic crime threat assessment, personal security vulnerability assessment, etc.).

The processes captured by these models are essential to the entire DTIM process and influence subsequent success in later phases. It is critical that the threat is well

defined and priorities established through essential elements of criminal information or priorities of intelligence requirements. Likewise, the DTIM process must be carefully managed to ensure that violations during the domestic intelligence process in phase I do not generate subsequent or more serious violations in later phases. The worst possible outcome might be the dismissal of a government case against a dangerous threat group, which, consequently, would no longer lack the opportunity of a second attempt.

As a final note, DTIM processes in phase I of the DTIM Model should heed the caution provided in appendix A of JP 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*. Its advice is borrowed from a similar context and is certainly applicable to the area of domestic intelligence management. The DTIM models discussed in sections I and II could conceivably provide

> the commander with a tool to assess the potential vulnerability of [or threat against] a base, unit, ship, or port activity, but it is [they are] not a substitute for sound judgment. These guidelines also serve to limit the scope of [DTIM] operations and are only one part of the larger issue that clearly and appropriately belongs to the traditional commanders' responsibilities for the overall well-being of service members, civilian employees, and family members as well as facilities and equipment.[41]

---

[1]Christopher Marlow, *Tamburlaine the Great*, 1587, Act ii, scene 2.

[2]US Army Command and General Staff College, ST 3-0, *Operations* (Fort Leavenworth, KS: USACGSC, October 2000), chapters 9-10.

[3]US Department of the Army, FM 101-5-1, *Operational Terms and Graphics* (Washington DC: US Government Printing Office, September 1997), 1-69.

[4]FM 101-5-1, 1-138.

[5]US Department of the Army, FM 100-23, *Peace Operations* (Washington, DC: US Government Printing Office, December 1994), 16.

[6]US Department of the Army, FM 100-8, *The Army in Multinational Operations* (Washington, DC: Department of the Army, November 1997), 3-0.

[7]FM 100-23, 37.

[8]Joint Chiefs of Staff, JP 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism* (Washington DC: US Government Printing Office, March 1998), D-1 and E-1.

[9]FM 101-5-1, 1-69.

[10]ST 3-0, 1-8.

[11]Ibid., 1-8.

[12]FM 101-5-1, 1-138.

[13]JP 3-07.2, II-2.

[14]Rick Maze, "Military a Step Closer to Domestic Terrorism Battle," *Navy Times*, 6/19/95, Vol. 44, Issue 37, 9.

[15]JP 3-07.2, GL-5.

[16]Ibid., II-11.

[17]Ibid., II-11.

[18]Carolyn W. Pumphrey, ed., *Transnational threats: Blending Law Enforcement and Military Strategies*, "Terrorism by Weapons of Mass Destruction: A Reassessment of the Threat," by Bruce Hoffman, (Washington DC: Strategic Studies Institute, 2000), 89.

[19]Ibid., 89-90.

[20]JP 3-07.2, III-4.

[21]Ibid., V-7.

[22]US Department of the Army, US Marine Corps, FM 100-19, FMFM 7-10, *Domestic Support Operations* (Washington DC: US Government Printing Office, July 1993), 3-5.

[23]Ibid., 3-5.

[24]US Department of the Army, U.S. Army Criminal Investigation Command, Operations Memorandum 002-00, *Force Protection Initiatives and Domestic Threat Intelligence*, (Fort Belvoir, VA: USACIDC, February 2000), B-1.

[25]State v Nelson (1979) 298 NC 573, 260 SE2d 629, cer den (1980) 446 US 929, 64 L Ed 2d 282, 100 S Ct 1867.

[26]United States v Red Feather (1975, DC SD) 392 F Supp 916.

[27]United States v Stouder (1989, MD GA) 724 F Supp 951.

[28]United States v Bacon (1988, CA11 GA) 851 F2d 1312.

[29]Riley v Newton (1996, CA11 GA) 94 F3d 632, 10 FLW Fed C 349.

[30]United States v Brown (1980 NCMR) 9 NJ 666.

[31]People v Burden (1979) 94 MI App 209, 288 NW2d 392, revd (1981 411 MI) 56, 303 NW2d 444.

[32]United States v Hutchings (1997, CA10 Utah) 127 F3d 1255, 97 Col J C A R 2426.

[33]United States v Del Prado-Montero (1984, Puerto Rico) 740 F2d 113, cert den (1984) 469 US 1021.

[34]Jackson v State of Alaska, (Date Not Found, AL) 22 Cr L 2338.

[35]United States v Walden (1974, CA4 VA) 490 F2d 372.

[36]Riley v Newton.

[37]State v Nelson (1979, NC) 298 NC 573, 260 SE2d 629.

[38]State v Trueblood (1980, NC) 46 NC App 541, 265 SE2d 662.

[39]Mathew J. Gilligan, "Opening the Gate," *Military Law Review*, Vol. 161, September 1999, 22.

[40]FM 100-19, B-1.

[41]JP 3-07.2, A-1

CHAPTER 5

CONCLUSIONS, RECOMMENDATIONS, AND FUTURE RESEARCH

> Every age [has] had its own kind of war, its own limiting conditions, and its own peculiar preconceptions[1]
>
> Carl von Clausewitz, *On War*

Introduction

This chapter provides some observations concerning the outcome of research into the Army's role in DTIM. It is divided into three major sections: strategic considerations, conclusions and recommendations, and suggestions for future research. The first section addresses the question of "What is next?" It includes some areas not specifically addressed in other chapters, but worth considering in summary. It considers the basic question of whether or not the Army should have a role in DTIM and, if so, what that role is. It reviews the current limitations imposed by Posse Comitatus and provides some insight into current trends that are forcing legislators, courts, and commanders to reexamine its application. Conclusions in this section focus on the Army's strategic role in civil-military operations and more specifically, it role in law enforcement and DTIM.

The second section provides conclusions and recommendations across those areas discussed in chapter 4. It provides some groundwork for commanders of domestic installations who are becoming increasingly involved in areas of interest that extend beyond their traditional boundaries. Perhaps the most important conclusions and recommendations involve the use of standard definitions and systematic processes as provided by the models at figures 3 and 4 for determining domestic threats and legally conducting domestic threat intelligence. This section also discusses a need for improved visibility over court findings and legal interpretations with respect to domestic civil-

military law enforcement and the benefits of collaboration between installation law enforcement and its legal advisors, as well as between the Army and the other services in achieving this visibility.

Finally, the third section discusses some unanswered questions and makes some recommendations for future research. Without question, DTIM is an emerging area that is still relatively incomplete, parochial, and fragmented. The objective of this section is to consider those areas that might provide a more complete picture of DTIM. What future research, for instance, might provide answers or solutions that will help consolidate and standardize DTIM operations? Also, what areas of research might provide the information necessary to develop or improve systems or processes to make DTIM operations more viable and effective? Finally, this section discusses a need for future research to test some of the ideas presented in chapter 4. How realistic are the concepts presented in the new threat and legal models at figures 3 and 4? What type of research approaches might be used to test the reliability and validity of these two models?

Section I. Strategic Considerations

The DTIM process as developed and discussed in this paper is a military law enforcement activity, with emphasis on the military. As such, it must always be kept in its proper perspective. DTIM is clearly a mission that operates in the gray area between those activities sanctioned, on one side, by executive emergency powers, military purpose doctrine, and the installation commander's inherent authority, and those activities, on the other side, that are expressly forbidden by the Posse Comitatus Act. Consequently, military law enforcement organizations conducting DTIM must always strive to define, articulate, and follow only those activities characterized by a clear military nexus.

Any conclusions and recommendations concerning DTIM must at least consider the latest changes or trends with respect to US laws and the military regulations that implement those laws. A true appreciation for these changes can only be understood within the historical and traditional context of the Posse Comitatus Act. While this Act generally prohibits use of the military for domestic assistance and particularly, for civil law enforcement, its provisions are both complex and dynamic. Its passage in 1878 did not overwrite constitutional authority or those laws enacted to support such constitutional influences. Under executive emergency authority, the President can and has called upon the Army numerous times in the almost 125 years since its passage to provide assistance for the enforcement of civil rights, to assist civil authorities during natural disasters, and even to provide law enforcement against national, state, and local civil demonstrations.

In recent years, too, the traditional separation between military and civil assistance has waned under the Army's increasing role in domestic support operations. Without question, the Army operations tempo has increased dramatically to accommodate this category of missions. In fact, it has participated in almost every natural disaster relief operation since 1980, supported civil law enforcement during the LA riots, assisted US Customs and the US border patrol in counterdrug operations, and even provided assets for the consequence management process following the Oklahoma City bombing incident.

Participation in other operations outside the domestic theater has also sparked the imagination of civil and military leaders to the possibilities of this new role. Doctrine covering OOTW scenarios has demonstrated the parallels between stability and support operations at home and abroad. It is no surprise, then, that doctrine covering these types

of operations, both at home and abroad, has continued to treat them similarly. Following the introduction of the term in FM 100-5 in 1993, doctrine covering these operations referred to them as stability and support operations, and, most recently only changed slightly to stability operations and support operations in the draft ST 3-0.[2]

As a result of these trends, the issue of whether or not to extend the authority of the military to directly assist civil authorities and, if so, to what extent, has been addressed on numerous occasions by the legislature. This issue finds proponents on both sides waving banners of legal dogma, traditions, and perhaps even a white flag from those who feel the military may be the only solution to stemming the tide of domestic threats. The debate presents the executive and legislative branches with a difficult dilemma that has emotional ties dating back even before its constitutional roots, originating from an eighteenth century mistrust of a large standing British Army among the early American colonies. This sentiment was reinforced numerous times when the military was used to squelch local rebellions, culminating in the US Army's constabulary role during the reconstruction era in the South, following the American Civil War.

The crux of the issue concerns the balance between providing national security and protecting the civil rights of US citizens. In other words, to what degree can the military be used to intrude into American lives for the sake of protecting them against domestic and transnational threats? On one side, the view of proponents for tradition was summed up during a 1995 debate on the senate floor: "Separation of military from civilian powers is rooted in our history, said Sen. Larry Craig, R-Idaho. We have cautiously and appropriately guarded that separation throughout our country's existence."[3] On the other side, however, a series of exceptions to this act, including the

1981 exception for assistance against drug trafficking, the 1982 exception for assistance in the event of a nuclear detonation on American soil, and the 1995 update of the latter, to provide assistance against terrorism and threats of chemical and biological use, provides a narrowly defined set of situations in which the military can be used.

Whether or not these exceptions grant substantial permission for military involvement in civil law enforcement, they bode of a trend in that direction. A 1986 article in the *Bulletin of the Atomic Scientist* predicts the possibilities:

> Despite the 1878 Posse Comitatus Act which prohibits use of US armed forces for ***domestic law enforcement***, the congress, in 1981, made an exception to that act allowing the Department of Defense to get involved in stemming illegal drug traffic. This opened the door for the Department of Defense involvement in other *law enforcement* operations as well.[4]

Indications of this trend have not escaped the military either. As mentioned earlier, the possibilities of military involvement in domestic affairs is captured in the latest military doctrine. Although currently unapproved, ST 3-0 separates traditional OOTW scenarios into two fronts: stability operations, which focus on the more traditional OOTW scenarios abroad, and support operations, which focus more on military operations in support of US civil authorities. Although this is not intended as an extension of military purpose doctrine, it is recognition of sorts of the Army's changing role on domestic front and of some subsequent changes that are gradually legalizing that area. Civilians alone do not contend this change in the Army's role; the following excerpt captures a tone of reluctance from at least one US Army War College student:

> It would appear that the national security of Engagement and Enlargement has opened the possibility of developing an entangling alliance between military forces oriented on external threats and police forces oriented on ***domestic*** security and ***law enforcement*** by coming closer and closer to crossing the line drawn by the PCA [Posse Comitatus Act]. Routine and recurring military support to

> civilian ***law enforcement*** agencies can involve a gradual assumption of civil roles for the military which might erode both its apolitical nature and its technical skill.[5]

If it indicates nothing else, the debate concerning the Posse Comitatus Act in recent years provides two important conclusions: first, issues surrounding the Army's role in the domestic environment are sensitive, and, second, Americans are concerned over potential effects of domestic threats. Both are inextricably tied and under current trends will continue to cause political friction. In the meantime, the Army will undoubtedly continue to provide domestic support operations as an instrument of executive powers, just as the legislature will probably continue to debate its future role in homeland defenses.

Whether or not the Army's role expands to include other tasks associated with the homeland defense, it must at least provide defenses for its own installations as part of the overall homeland defense. Army installations must be capable of resisting the effects of threats, which, if successful, could only increase public fear, erode valuable resources and capabilities, and strengthen the power and resolve of targeting threat groups. Of all the adverse effects, it is perhaps public fear that could be affected the most by threat activities against Army installations. As a symbol of American strength and defense, Army installations present an extremely high symbolic value as a potential target of domestic threats. Consequently, in every account following a threat strike, the actions taken by the installation commander to prepare against threats, like those of the USS *Cole*, will be publicly scrutinized.

In the final analysis, commanders must address the same questions, at least rhetorically, that William Natter refers to as "accountability to the unreasonable," when

Americans ask those accountable for protecting the homeland or protecting their sons and daughters:

> What is being done? What assurances do we have? How much money has been spent? And, perhaps the most significant question, have we as a nation done everything possible? To a member of Congress, they ask, "have you done everything **conceivably** possible?" This last question leaves representative and senators vulnerable if, heaven forbid, something catastrophic occurs.[6]

The commanders' inherent responsibility to protect the Army installations presents a final area affected by the Posse Comitatus Act. As discussed earlier, this act does not prevent military law enforcement activities beyond the installation boundaries. It only prevents the military from conducting law enforcement activities in direct support to civil authorities, where civil support is the primary motive for the activity. Whether or not commanders improve security vigilance to the full parameters of their areas of interest will depend on their understanding of the provisions established under military purpose doctrine and what they feel is within their inherent authority to defend the installation against domestic threats.

Section II. Conclusions and Recommendations

For the Army, Natter's rhetorical question presents a compelling argument for standardizing its domestic threat doctrine and sorting through the legal implications of conducting DTIM within its areas of interest. The first task suggests that the Army must provide a standard threat model that will accommodate the full threat spectrum, including the most dangerous, as well as the most likely scenarios. The Army must reevaluate its overemphasis on terrorism for a more evenhanded approach that considers the pervasiveness and frequency of a threat, and not just its potential effects.

As discussed in chapter 4, a standard threat model will ensure that threat analyses across all installations and the subsequent threat reports are standardized, as well as ensure that resources and crisis response decisions are based on the measurable differences between local circumstances and conditions. A threat model, like the one presented in figure 3, will help provide installations with standard metrics to evaluate threat groups and to focus DTIM operations. It will ensure that a threat score of seven at one installation is similarly based and equal to a seven at another installation, and that both are less serious than a threat receiving a rating of ten at still another installation. Likewise, any given installation should characterize one threat group the same as any other installation. This standardization also provides continuity between installation law enforcement and force protection agencies and between the installation and local civil authorities for collaboration.

To fully answer the question, "Have you done everything **conceivably** possible?" the Army must also accomplish the second task.[7] Through its commanders, in conjunction with their staffs, it must provide clear and progressive guidance with regard to conducting law enforcement and DTIM operations within the constraints of legitimate exceptions to the Posse Comitatus Act. To accomplish their inherent responsibility to protect the installation and its associated force protection objects, commanders must be provided a view beyond their immediate boundaries; they must be allowed to conduct the intelligence necessary to anticipate domestic threats.

Law enforcement operations stemming from the installation commanders inherent authority to maintain law and order on the installation are permissible. Consequently, those actions necessary to accomplish those operations are also permissible. Even off the

installation, “the Military Purpose Doctrine generally will permit . . . actions that support a legitimate military purpose” and “where a legitimate, independent military purpose exists, military law enforcement officials are authorized to conduct activities . . . . In other words, when off-post criminal activity adversely impacts the welfare of persons and the efficiency of operations on post, a legitimate, independent military purpose exists.”[8]

To promote but justify DTIM operations, the Army must provide more definitive guidance on determining the military nexus between off-post threats and their adverse impact against installation interests. Here, too, the DTIM Legal Assessment Model at figure 4, or something similar, could be used to provide a systematic process whereby all essential elements for determining the nexus would be considered. Moreover, such a model would help standardize DTIM operations across all continental US installations, and provide many of the same subsequent benefits as the Domestic Threat Assessment Model. A standard legal model would offer two additional benefits: first it would assist military law enforcement in defining and articulating the military nexus behind its activities and second, it would provide a standard training platform for military law enforcement personnel. Both benefits might provide a more productive dialogue between law enforcement and installation legal advisors to assist with defining the military nexus.

The notion that using these models might provide a common language among different installations is a powerful one. It would provide installations the ability to collaborate without diminishing their flexibility to tailor their DTIM operations to a specific threat or legal environment. This common language could also act as a forum from which to develop or improve doctrine. At the most obvious level, the models’ worksheets provide both continuity and a source for further inquiry without the added

liability of intelligence against specific persons or organizations. Less obvious perhaps is the advantage they provide for managing change. They provide a platform that is easily evaluated, one that would accommodate additional variables or improvements in metrics. Also, adopting these kinds of systems or processes now may offer a slate for writing subsequent changes at the strategic and operational levels.

One caveat to using these models or any other system, however, is provided by FM100-19, *Domestic Support Operations*, and should always remain at the top of the installation's DTIM checklist:

> Laws governing use of the military in domestic operations are complex, subtle, and ever-changing. For this reason, commanders should discuss plans, policies, programs, exercises, funding, and operations with their legal advisors.[9]

Finally, the Army must also increase its visibility of crimes, as they pertain to the military purpose doctrine and the installation commanders' inherent authority, through the entire adjudication process. Court findings and legal interpretations are continuously building legal precedence with regard to installation law enforcement and force protection. This precedence must be collected, collated, analyzed, and where appropriate, integrated into current law enforcement and security planning and operations. This process should include the same law enforcement, legal, security and other functional advisors who are responsible for installation security and who normally sit on the force protection council, but at a minimum, should at least include law enforcement and legal advisors.

At the higher levels too, the Army should develop a formal process to improve its cognizance of those changes occurring in the civil and military court systems affecting the other services. A joint committee representing the services, for instance, could

provide insight into the lessons learned through an analysis of their respective appellate court findings or legal interpretations. Such information would undoubtedly assist each service because "Congress has enacted statutes requiring the military departments to protect military installations and property," and with the exception of the Coast Guard, the Posse Comitatus Act affects all and, certainly, all including the Coast Guard are affected by domestic threats.[10] It would help standardize law enforcement and DTIM procedures DoD wide, as well as providing the benefits of synergy.

Section III. Future Research

Because DTIM is a relatively new emerging area, there is much that can be researched to fill in some of the holes and gaps with respect to current doctrine and to establishing of some fundamental data to support current processes and recommendations. Accordingly, this section discusses those areas where future research might prove productive. Although the discussion does not trace a specific outline, it will cover areas starting from more strategic and philosophical recommendations and proceed to those that are more operational and applicable to this thesis.

The first recommendation is to explore the doctrinal similarities and differences in providing law enforcement and security measures between stability operations and domestic operations. It appears that law enforcement, security, and force protection operations in the domestic environment may parallel those being conducted in support of stability operations. During stability operations there may not be a defined enemy, but these are still adversaries. In these environments aggression may routinely take the form of criminal acts rather than formal enemy operations. This is similar and, in fact, parallels domestic operations in that threats may fall along the threat spectrum from

unsophisticated criminals to terrorist. This may also be true in combat operations at the higher end of the operational spectrum. In combat operations criminal acts, however threatening, may take a back seat to the main effort, but as the theater matures and enemy combat power is reduced, security activities and force protection will probably become increasingly more focused on countering criminal activity similar to a domestic environment.

The next area for future research focuses on more strategic DTIM related activities in the joint arena to establish a basis for conducting similar Army DTIM operations. Here, future research might compare trends between the armed services in three areas: (1) a comparison study of law enforcement and DTIM, (2) a comprehensive study of appellate court findings and legal interpretations regarding military-civil law enforcement and DTIM, and (3) a study of trends regarding military assistance to civil authorities that is provided as an exception to Posse Comitatus. Each of these areas would provide insight from a broader perspective than the Army's alone. Since the services, as discussed earlier, must all provide installation or base protection in the continental US and since the same laws and similar regulations equally affect them, this research may provide some collective insight and synergy for developing and improving current systems and processes.

The next area of research might focus on measuring the accumulative adverse effects on installations from each of the different threat groups. This would provide some insight into the effects from the most dangerous versus the most likely threat scenarios. For instance, what are the cumulative effects on installations from threat groups that are more pervasive and strike more frequently, such as drug traffickers and gangs, as

opposed to the effects on installations from the potentially more dangerous threat groups, such as extremists and terrorists? This research might address a possible oversight in the Army's approach to its threat doctrine, as well as address the overemphasis in joint doctrine on terrorism as the primary domestic threat. It may even answer questions concerning the probability of a threat group transitioning into another threat group.

Findings from this research might also be used to evaluated the Domestic Threat Assessment Model at figure 3. It could potentially answer some of the following questions: (1) Does the list of threats include the appropriate threat groups? (2) Are the threat groups ranked in the appropriate order? and (3) Are the metric weightings assigned to each threat group appropriate, based on their adverse effects?

Similarly, future research might directly address the validity and reliability of the Domestic Threat Assessment Model. Research could test these components by using either real criminal data or fabricated scenarios using realistic crime data to determine if the assigned metrics are proportionate to the actual threat. This type of method would also allow a comparison of the model against similar threats to see if scores remain constant or, in other words, reliable. Finally, this method might bring to light other elements that may not be included in the model, but nevertheless, affect a realistic point assessment.

More research for testing the validity and reliability of models leads to a final recommendation for future research. A method similar to the one recommended for the Domestic Threat Assessment Model could also be used to test the validity and reliability of the DTIM Legal Assessment Model. Again, researchers could provide scenarios using either real or at least realistic criminal data to validate the model. Methodology would

hinge on successfully developing a series of scenarios that consist of multiple variables including those listed in the model, and any others that can be identified. Research could then test the validity of each variable and its conditions independently and then their validity when combined with other variables. This methodology could confirm or deny the inclusiveness of the current set of variables and conditions. It would also validate the metric system for each variable condition, as well as the reliability by confirming similar scores when tested against similar situations.

Conclusion

The recommendations and conclusions presented in this chapter, as well as those discussions included in the preceding chapters, are by no means inclusive or even definitive in nature. They represent only a single view regarding the extremely complex and ever-changing area of DTIM. This thesis, rather, is meant to broaden the current perspective toward conducting DTIM and DTIM-related activities and to point out and discuss areas affecting its development. Although the Army can neither predict the changes in laws nor the twists and turns presented in case law, it can actively compile, assess, and integrate the current laws, legal exceptions, and subsequent interpretation of those laws by the courts in order improve DTIM operations. Whether this endeavor meets the priority threshold in an environment of increasing operations tempo or not, current trends indicate that the potential for domestic threats against continental US Army installations is on the rise, that Americans and their congressional representatives are concerned about domestic threats, and that the inherent responsibility of commanders to protect their installation grows more acute. As a final note, JP 3-07.2 provides the

bottom line for initiating improvements in this area: "An effective intelligence and counterintelligence program is essential in order to identify the . . . threat."[11]

---

[1]Carl von Clausewitz, *On War*, edited by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 593.

[2]US Department of the Army, FM 100-5, *Operations* (Washington, DC: Department of the Army, June 1993), chapter 13.; and US Department of the Army, Command and General Staff College, Student Text 3-0, *Operations* (Fort Leavenworth, KS: USACGSC, October 2000), chapter 9 and 10.

[3]Rick Maze, "Military a Step Closer to Domestic Terrorism Battle," *Navy Times* 44, no. 37 (19 June 1995): 9.

[4] "Department of Defense Involved in Law Enforcement," *Bulletin of the Atomic Scientists*, February 1986, 4.

[5]J. G. Diehl, *Cop and the Soldier: An Entangling Alliance: The Posse Comitatus Act and the National Security Strategy of Engagement and Enlargement* (Carlisle Barracks, PA: US Army War College, April 97), 72.

[6]Carolyn W. Pumphrey, ed., *Transnational threats: Blending Law Enforcement and Military Strategies*, William Natter, "Terrorism and National Defense: The Congressional Perspective" (Washington DC: Strategic Studies Institute, 2000), 232.

[7]Mathew J. Gilligan, "Opening the Gate," *Military Law Review* 161 (September 1999): 21.

[8]Ibid.

[9]US Headquarters, Department of the Army, US Marine Corps, FM 100-19, FMFM 7-10, *Domestic Support Operations* (Washington DC: US Department of the Army, July 1993), 3-1.

[10]"Opening the Gate," 13.

[11]Joint Chiefs of Staff, JP 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism* (Washington DC: US Government Printing Office, March 1998), X.

BIBLIOGRAPHY

Periodicals and Articles

Carter, Ashton, John Deutch, and Philip Zelikow. "Catastrophic Terrorism: Tackling the New Danger." *Foreign Affairs* 77, no. 6 (November-December 1998): 80-94.

Cohen William S. "Preparing for a Grave New World." *The Washington Post*, 26 July1999, A19.

Danzig, Richard. "Biological Warfare: A Nation at Risk--A Time to Act." *Strategic Forum* 58 (January 1996): 1-5.

Ember, Lois R. "FBI Takes Lead In Developing Counterterrorism Effort." *Chemical and Engineering News* 76, no. 46 (4 November 1996): 10-18.

Gilligan Mathew J. "Opening the Gate," *Military Law* Review 161 (September 1999): 1-56.

Hoffman, David. "Suitcase Nuclear Weapons Safely Kept, Russian Says." *The Washington Post*, 14 September 1997, A23.

Maze Rick, "Military a Step Closer to Domestic Terrorism Battle." *Navy Times* 44, no. 37 (19 June 1995): 9.

Mylroie, Laurie. "The World Trade Center Bomb: Who is Ramzi Yousef? And Why It Matters." *The National Interest* 42 (winter 1996). Document on-line. Available from http://www.fas.org/irp/world/iraq/956-tni.htm. Internet. Accessed 15 August 2000

"Department of Defense Involved in Law Enforcement," *Bulletin of the Atomic Scientists,* (February 1986), 4.

Government Documents and Sources

Chairman of the Joint Chiefs of Staff. Chairman of the Joint Chiefs of Staff Instruction 3214.01, *Military Support to Foreign Consequence Management Operations*. Washington, DC: Department f Defense, 1998.

_____. Joint Publication 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*. Washington, DC: Department of Defense, 1998.

Cohen, William S. *Report of the Quadrennial Defense Review*. Washington, DC: Department of Defense, March 1997.

Cordesman, Anthony. Defending America: Redefining the Conceptual Boarders of Homeland Defense. Homeland Defense: Coping with the Threat of Indirect,

Covert, Terrorist, and Extremist Attacks with Weapons of Mass Destruction (Draft). Washington, DC: Center for Strategic and International Studies, 2000.

Defense Special Weapons Agency. DSWA Publication DSWA-AR-40H, *Weapons of Mass Destruction Terms* Handbook. Alexandria, VA: Defense Special Weapons Agency, 1998. Department of Defense Tiger Team. "Department of Defense Plan for Integrating

National Guard and Reserve Component Support for Response to Attacks Using Weapons of Mass Destruction." 1998. Document on-line. Available from http://www.defenselink.mil/ pubs/wmdresponse/. Internet. Accessed 14 October 2000.

Federal Bureau of Investigation. *Weapons of Mass Destruction Incident Contingency Plans (WMDICP)*. Washington, DC: Federal Bureau of Investigation, National Security *Division*, Domestic Terrorism/Counterterrorism Planning Section, 1998.

Diel, J. G. *Cop and the* Soldier*: An Entangling Alliance. The Posse Comitatus Act and* the National Security Strategy of Engagement and Enlargement. Carlisle, PA: U.S. Army War College, April 97.

Federal Emergency Management Agency. *Terrorism Incident Annex*. FEMA Webpage,

2000. Document on-line. Available from http://www.fema.org/r-n-r/frp/ frpterr.htm. Internet. Accessed 6 October 2000.

Frostic, Frederick L. Quoted in Earl H. Tilford, Jr., *National Defense into the 21st Century: Defining the Issue*. Carlisle, PA: U.S. Army War College Strategic Studies Institute, 1997.

Larson, William Jed. "Chemical and Biological Weapons: A Growing Problem for the CINC." Thesis, Naval War College, 1997.

Public Law 93-288. Disaster Relief Act. U.S. Code. Vol. 1, secs. 101-606 (1974).

Public Law 104-201 Title XIV. Defense Against Weapons of Mass Destruction. U.S. Code. Vol. 2, secs. 1401-1455 (1996).

Pumphrey, Carolyn W. *Transnational threats: Blending Law Enforcement and MilitaryStrategies*. Washington DC: Strategic Studies Institute, 2000.

U.S. Army. Deputy Chief of *Staff* of Operations. "Homeland Security (HMS) Army Strategic Plan, Initial Distribution Draft." 18 October 2000.

_____. Training and Doctrine Command. Supporting *Homeland Defense.* WhitePaper, May 1999. Document on-line. Available from

http://www.fas.org/spp/ starwars/program/homeland/final-white-paper.htm. Internet. Accessed 14 October 2000.

U.S. Congress. Senate. Oversight Subcommittee of the House Transportation Committee. U.S. Representative Tillie Fowler (R-FL) Holds Hearing on Terrorist Defense. 106th Congress, 2nd Session, 6 April 2000.

U.S. Department of the Army. Field Manual 1910, *Law Enforcement Operations*. Washington, DC: Department of the Army, 1987.

_____. Field Manual 100-5, *Operations*. Washington, DC: Department of the Army, 1993.

_____. Field Manual 100-19 (Fleet Marine Force Manual 7-10), *Domestic Support Operations*. Washington, DC: Department of the Army, 1993.

_____. Field Manual 100-23, *Peace Operations*. Washington, DC: Department of the Army, 1994.

_____. Field Manual 101-5-1, *Operational Terms and Graphics*. Washington, DC: Department of the Army, 1997.

_____. Regulation 190-13, Physical *Security: The Physical Security Program*. Washington, DC: Department of the Army, 1993.

_____. Regulation 195-2, *Criminal Investigation Activities*. Fort Belvoir, VA:USACIDC, 1985.

_____. Regulation 190-30, *Military* Police *Investigations*. Washington, DC: Department of the Army, 1978.

_____. Regulation 210-10, *Installation Administration*. Washington, DC: Department of the Army, 1977.

_____. Regulation 500-51, *Support to Civilian Law Enforcement*. Washington, DC: Department of the Army, 1983.

_____. U.S. Army Command and General Staff College, *National Military Strategy*. Fort Leavenworth, KS: USACGSC, August 2000.

_____. U.S. Army Command and General Staff College, Student Text 3-0, *Operations*. Fort Leavenworth, KS: USACGSC, October 2000.

_____. U.S. Army Criminal Investigation Command Operations Memorandum 002-00, *Force Protection Initiatives and Domestic Threat Intelligence Management*. Fort Belvoir VA: USACIDC, February 2000.

_____. U.S. Army Military District of Washington Homepage. Document on-line. Available from http://www.mdw.army.mil. Internet. Accessed 5 February, 2001.US Department of Defense. Department of Defense Directive 3025, *Military Assistance For Civil Disturbance*. Washington, DC: Department of Defense, 1994.

_____. Department of Defense Directive 5200.8, *Security of Military Installations*. Washington, DC: Department of Defense, 1991.

_____. Department of Defense Directive 5200.27, Acquisition of Information Concerning Persons and Organizations Not Affiliated with theDepartment of Defense. Washington, DC: Department of Defense, 1980.

_____. Department of Defense Directive 5525.5, *Cooperation with Civilian Law Enforcement Officials*. Washington, DC: Department of Defense, 1986.

_____. Inspector General Policy Memorandum, *Crimnal* Drug *Investigative Activities*. Washington, DC: Department of Defense, 1 October 1987.

U.S. Department of State. "Patterns of Global Terrorism 1999." Department of State Publication 10687, Washington, DC, April 2000. Database on-line. Available from http:// www.state.gov/www/global/terrorism/1999report/1999index.html. Internet. Accessed 17 October 2000.

U.S. President. Presidential Decision Directive 39, *U.S. Policy on* Counterterrorism, 21 June 1995. Document on-line. Available from http://www.fas.org/irp/offdocs/ pdd 39.htm. Internet. Accessed 6 October 2000.

_____. Presidential Decision Directive 62. *U.S. Policy on* Combating *Terrorism*, 1998. Document on-line. Available from http://www.fas.org/irp/off docs/pdd39.htm. Internet. Accessed 10 October 2000.

The White House. *A National Security Strategy for a* New *Century*. Washington, DC:The White House, December 1999.

United States Code and Case Law

Title 5, USCS. 301 (1998).

Title 10 USC, 375. (1998).

Title 18 USC, 1385 (1986).

Jackson v State of Alaska, (1991, AL) 22 Cr L 2338.

People v Burden (1979) 94 MI App 209, 288 NW2d 392, revd (1981 411 MI) 56, 303 NW2d 444.

Riley v Newton (1996, CA11 GA) 94 F3d 632, 10 FLW Fed C 349.

State v. Harker (1983, AK) 663 P2d 932, 936.

State v Nelson (1979 NC) 298 NC 573, 260 SE2d 629, cer den (1980) 446 US 929, 64 L Ed 2d 282, 100 S Ct 1867.

State v Taylor (1982, OK) 645 P2d 522.

State v Trueblood (1980, NC) 541, 265 SE2d 662.

United States v Del Prado-Montero (1984, Puerto Rico) 740 F2d 113, cert den (1984) 469 US 1021.

United States v Bacon (1988, CA11 GA) 851 F2d 1312.

United States v Brown (1980 NJ) 9 NJ 666.

United States v Hutchings (1997, CA10 UT) 127 F3d 1255, 97 Col J C A R 2426.

United States v Red Feather (1975, DC SD) 392 F Supp 916.

United States v Stouder (1989, MD GA) 724 F Supp 951.

United States v Walden (1974, CA4 VA) 490 F2d 372.

Other Sources

Clausewitz, Carl von. *On War*. Edited by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976, 593.

Marlow, Christopher. *Tamburlaine the Great*. 1587, Act ii, scene 2.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
   U.S. Army Command and General Staff College
   250 Gibbon Ave.
   Fort Leavenworth, KS 66027-2314

2. Defense Technical Information Center/OCA
   8725 John J. Kingman Rd., Suite 944
   Fort Belvoir, VA 22060-6218

3. MAJ Charlotte Herring
   LID
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

5. LTC Mark A. Beattie
   DJMO
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

6. Dr. Harold Orenstein
   CADD
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 1 June 2001

2. Thesis Author: MAJ Mark A. Jackson

3. Thesis Title: Domestic Threat Intelligence Management

4. Thesis Committee Members _____

   Signatures: _____

   _____

   _____

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

A B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

EXAMPLE

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
Direct Military Support (10)	/	Chapter 3	/	12
Critical Technology (3)	/	Section 4	/	31
Administrative Operational Use (7)	/	Chapter 2	/	13-32

Fill in limitation justification for your thesis below:

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
	/		/	
	/		/	
	/		/	
	/		/	
	/		/	

7. MMAS Thesis Author's Signature: _____

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).